International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 13, No.1 (Jan-2023)

http://dx.doi.org/10.12785/ijcds/130109

Securing the Internet of Things Through Blockchain Approach: Security Architectures, Consensus Algorithms, Enabling Technologies, Open Issues, and Research Directions

Sadia Showkat[1] **and Shaima Qureshi**[2]

[1]*Department of Computer science and Engineering, National Institute of Technology Srinagar, J&K*
[2]*Department of Computer science and Engineering, National Institute of Technology Srinagar, J&K*

Received 25 Oct. 2021, Revised 5 Jan. 2023, Accepted 12 Jan. 2023, Published 31 Jan. 2023

Abstract: The rapid expansion of the Internet of Things (IoT), particularly in critical infrastructures, necessitates strict security and privacy standards. Owing to data proliferation, Cyber-physical systems (CPS) rely on computing platforms for the provision of services and resources. The futuristic “Beyond 5G” (B5G) enabled critical IoT infrastructures cannot run on centralized systems due to their security vulnerabilities that compromise the basic Confidentiality-Integrity-Availability (CIA) triad. Blockchain technology (BCT) is emerging as a key enabler in addressing IoT’s security challenges, and it is compliant with the Fog-IoT architecture. The Ethereum platform has ushered an unprecedented development in BCT by facilitating application development. Blockchain (BC) connects the users’ chain identity to the transactions associated with their tokenized digital assets and confers the ability to audit the system. The history of canonical transactions is recorded in an immutable fashion facilitating data tracking and deterrence of data repudiation. A Consensus mechanism (CM) governs the state transitions and the node behavior in building trust relationships between various entities in the absence of a central authority. Through Smart Contracts(SCs), distributed and trustworthy access control can be achieved for IoT systems besides enhancing automation. We argue that BCT adoption is inevitable in securing futuristic B5G enabled IoT critical infrastructures for ensuring flexible and fine-grained access control, authentication, communication, and data security. Various challenges are associated with their adoption, such as the rising cost of Ethereum and constraints in the IoT environment. To facilitate BC solutions for IoT security, the functionality of BCT must be complemented with other technologies such as Machine Learning (ML), Edge Computing (EC), and InterPlanetary Filesystem(IPFS).

Keywords: Blockchain, IoT, Edge Computing, Consensus, Security, Privacy, Smart contracts, IPFS B5G, Access control.

1. INTRODUCTION

The industry is rapidly evolving into a holistic network of intelligent systems capable of making data-driven decisions. Many technologies have aided this transition, with IoT being at the core. IoT connects devices and couples them to the internet forming a CPS. IoT is at the center of intelligent applications in and outside the industry. IoT offers the remote control and monitoring of equipment and catalyzes data-driven automated decision and action-taking capabilities, resulting in increased system efficiency and throughput while lowering costs. IoT is causing a major upward shift in the revenue pool, and its growth can be assessed by the increase in the number of practical applications across regions.

IoT enables a pervasive interconnection of virtual and physical objects for accelerated data sharing and collection. Sensing capabilities are embedded in intelligent devices such as smartphones, laptops, and fitness monitors, while intelligence is built into traditional sensors for extensive data monitoring. As per the Ericson report, by 2050, there will be 24 billion interconnected IoT devices [1]. The data streams are generated continuously with volumes reaching exabytes; thus, the data is referred to as IoT Big data. At present, Cloud Computing and Fog Computing are the most popular provisions to handle the high-end computing and storage demands of IoT big data [2].

IoT aims to create intelligent, unified, fully distributed, secure, and cost-efficient systems. Reliable storage, data awareness, ease of access, scalability, and channel security are important parameters while adopting a wireless system. IoT systems come with inbuilt security measures that can be bypassed due to their intrinsic traits.Various factors are responsible for hindering the pace of IoT security. These include:

1) Any end- end encryption technique employed to provide data security in networks is challenging to be embedded in IoT networks due to the constrained

E-mail address: sadia_01phd18@nitsri.net, shaima@nitsri.net.

nature of the devices.

2) IoT devices are lodged in uncontrollable, heterogeneous, complex, open, untrustworthy environments, which magnify the attack space.
3) Lack of standard architecture, a common addressing scheme limits the integration and replication of security measures from other IoT systems.
4) IoT is an ever-growing field, and the security features of constrained devices are not evolving at the same pace as the system itself.
5) The adoption of computing platforms forces frequent transfer of data. Implementing robust cryptographic algorithms is expensive and increases the overall cost of the system.
6) IoT systems communicate across different domains and require fine-grained Access control(AC) mechanisms for collaboration.

Cloud and Fog platforms are vulnerable to cyber-attacks and fail to meet the demand for flexible cross-domain interoperability across multiple systems with distributed resources. The Data Management (DM) systems are centralized and prone to hackers who can manipulate the database, thereby compromising data integrity. The overreliance on a centralized database causes the “Single point failure” problem. The monetary transactions require the intermediation of a third party, which incurs verification costs and increases privacy concerns. These centralized architectures are prone to security threats that disorder the regular operation of systems. These include Denial of Services(DoS), Distributed Denial of Services(DDoS), Ransomware attacks, Eavesdropping, Side-channel attacks, Spoofing, Routing attacks, Man in the middle attack, SQL injection, and Phishing [3].

With the advancement in B5G technology, IoT is set to transform the existing digital landscape, but its inadequate security features have limited its adoption. B5G mobile communication technologies aim to provide high-speed transmission network support and enormous access points to maximize IoT capabilities [4]. The security measures of such applications need enhanced security and efficient DM. BCT is emerging as a promising paradigm for bringing disruptions in IoT security and is highly compliant with the Fog-like system of architecture [5].

BCT has created a paradigm shift by enabling trusted and anonymous transactions. BCT establishes trust between the communicating nodes, and the decision-making is based on CMs suitable in distributed environments. Owing to its unique propensities– Immutability, Transparency, Traceability, Resilience, and Encryption, the adoption of BCT is suitable for the realization of futuristic peer-peer, trustless applications. BCT supports tokenized assets, and the nodes in the network interact automatically without the intervention of any central authority. This increases the privacy of the network and eliminates the management cost.

BCT is creating major reforms in IoT management and security. The IoT transactions are encrypted and secured using digital signatures and cryptographic keys. BCT eliminates the security threats with a distributed CM and provides a true system state upon which every legitimate user agrees. With the integration of BCT, IoT applications are becoming decentralized, transactions are trusted and anonymous, and cross-domain interaction is enhanced. The system security is increased through ownership records, encrypted transactions, distributed storage, consensus, and authentication mechanisms. Figure 1 illustrates the difference between a centralized and BC-based IoT system.

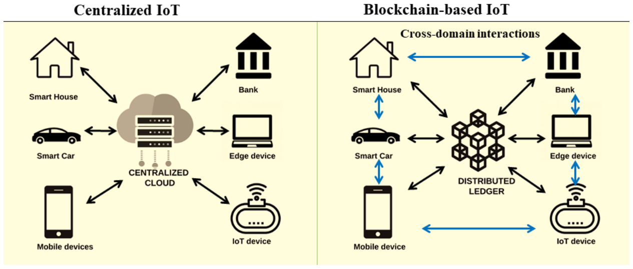


Figure 1. Centralized Vs. BC-based IoT

There are multiple challenges concerning the BC integrated IoT systems, such as network complexity, limited bandwidth, computation capabilities, data diversity, scalability, and throughput. Conventional CMs consume huge amounts of resources to slow down the access rate of new blocks and protect the BC network from attacks, which is too expensive for resource-limited IoT devices. Further, the capacity of a new block is limited, and transactions per second (TPS) are usually limited to 20 to 30 TPS in Ethereum, rendering the system unable to respond to the influx of transactions [6]. With tradeoffs between adversity tolerance, latency, and energy consumption, research on IoT suitable CMs is growing.

BC itself suffers from security and privacy issues. Implementing longer chains is challenging, and the SCs can prove to be a double-edged sword. The cost of Ethereum is rising continuously, making the storage and transactions expensive for large-scale adoption. The underlying technologies powering BCT consume high power and are not suitable for IoT. BCT can revolutionize IoT, but enabling technologies such as IPFS, ML and EC must be integrated with BC to outweigh its current limitations.

IPFS is a distributed file system that can resolve BC –IoT big data problems. Instead of storing the data on the chain, IPFS hashes identifying the files are kept in the BC. The hash on the BC assures that the file has not been tampered with. File hashes can be used to link files to their owners and access rights.Solving complex puzzles such as Proof of work consumes a significant amount of CPU time and energy, making it unsuitable for resource-constrained IoT nodes. EC enables edge devices to carry out data resource incentive transactions and can be leveraged for performing consensus. Information hidden in IoT big data can be harnessed by feeding them to ML models, producing more generalized results on big data.The integrity of the data can be maintained by feeding trustworthy data to ML through BC. Conversely, more security can be imparted into BC through ML.

BCT is regarded as a promising technology for IoT because it provides significant solutions for decentralized networks that address trust and security concerns. Although BC outperforms centralized solutions in network security, BC-IoT integration is still in its early stages of adoption. Many challenges such as cost, compatibility, and privacy issues hinder the widespread adoption of BC security solutions in IoT. To realize the full potential of BC-based IoT, exhaustive research is necessary for exploring the enabling technologies for BC in lightweight(LW) environments.

A. *Objective and Contribution*

This paper aims to provide a comprehensive overview of the potential and challenges of BC-based IoT security solutions and enabling technologies, open issues, possible solutions, and future research directions. There are four focal research points of our study, and are listed below-

1) Firstly, to highlight the problems in centralized-based IoT solutions and understand why shifting to BC-based solutions is necessary.
2) Since the robustness of a BC-based system is highly dependent on its underlying consensus mechanism, the aim is to conduct an in-depth comparative analysis of CMs that are IoT suitable.
3) Thirdly, to critically review the existing BC-based IoT security solutions in view of five IoT security tasks-
   a) Key Management and Access control.
   b) Device Authentication.
   c) Routing Security.
   d) Malware Prevention. and
   e) Data Protection and Secure Database Management.
4) Fourthly, to highlight the open challenges in the BC-IoT integration and list out key future research directions.

The main contributions of the paper are as follows:

1) We have conducted a thorough survey of recent surveys(2019-early 2022) on BCT applicability in IoT. Other researchers may find this pool useful as a starting point for their research.
2) We have discussed BC as a key enabling technology for IoT and three technologies that power BC-IoT.
3) We have reviewed CMs in light of IoT.
4) A primary literature review of the recent BC integrated IoT solutions in perspective of five specific IoT security tasks.
5) We have discussed the cost analysis of IoT storage through SCs, network traffic modeling, SC vulnerabilities, BC transactional privacy, and other challenges.
6) We have thoroughly discussed the open issues and presented strong research directions.

B. *Paper Organization*

The remainder of the paper is organized as follows. In Section 2, the scope of the survey is presented. Section 3 presents the security vulnerabilities of six critical IoT applications and lays the rationale for moving toward decentralized architectures. In Section 4, we briefly provide an overview of BCT, its architecture, and CMs. Section 5 presents the highlights of the recent surveys (2019-early 2022). Based on the study in section 5, we discuss BC as a key facilitator for IoT and technologies that accelerate BC adoption in IoT in Section 6. In Section 7, a detailed study of BC integrated IoT security architectures and a comparison of various CMs, their adoption, and tradeoffs is discussed. In section 8, a literature review of BC-based security solutions is presented. In section 9, we present a thorough overview of the challenges associated with BC adoption in IoT, point out the open issues and possible solutions, and suggest promising research directions

2. Scope of the survey

We begin our review with a study of the prevalent centralized IoT architectures and discuss their security vulnerabilities. We identify five primary security tasks, evaluate them against centralized solutions, and determine their limitations and the need to shift to decentralized solutions such as Blockchain. We then discuss the fundamentals of Blockchain. The working of the SCs have been excluded, and instead, their security vulnerabilities and applicability has been discussed. Considering the vastness of BC applicability, especially in IoT security, we shortlist a pool of recent survey papers (2019-early 2022) and comprehensively highlight their key focal points. The research papers have been shortlisted based on keywords, the number of times cited, and relevance to one of the five domains- General IoT security, IoT suitable CMs, BC-based IoT applications, BC for B5G applications, and integration with Machine Learning and BC- Edge computing. Other researchers may find this pool useful as a starting point for their research.

Based on our secondary survey, we broadly discuss the reason for merging BC with IoT, how BC is a key enabling technology for IoT and what technologies drive BC and mitigate the challenges associated with BC adoption in IoT. We have discussed three enabling technologies for powering BC adoption in IoT- EC, IPFS, and ML. We then discuss the BC-IoT integration in great detail and present the technicalities of BC adoption in IoT. Since a BC network is only as good as its consensus, we conduct a detailed comparative analysis of CMs in light of IoT goals and related tradeoffs. Based on the study, we shortlist IoT suitable CMs and BC platforms. We then review the recent BC-based IoT architectures and evaluate them against the previously identified security tasks. We have filtered a subset of research papers(2018-early 2022) where the focal points are specifically the five IoT security tasks mentioned in subsection 1(A). Each paper's experimental work and results have been carefully studied, and the aim, architecture, pros, and cons of each solution have been comprehensively summarized. Finally, based on the literature review of BC-

IoT architectures, we thoroughly discuss the challenges in BC-IoT integration and present research issues and future research directions.

3. Security vulnerabilities of Centralized IoT applications:

IoT's centralized architecture has three major network components-a) End devices: These are devices with sensing and actuating abilities coupled to the CPS. They amass data in the environment that they are lodged in and take action. b) Gateways and Data acquisition systems (DAS): DASs acquire data from sensors, and the gateways enable the Device-Cloud interactions working on different network protocols. c) Computing platforms: The data is relayed to platforms that provide storage, processing, hardware, software, and analytical support to the system.

A. *IoT Goals*

IoT architecture must satisfy the following primary goals:

1) Low Power consumption: IoT devices are constrained and require low-powered communication protocols to increase the network's lifetime.
2) Adaptability: The addition of new devices, frequent changes in the network conditions, and mobility of devices are essential factors in an IoT network. IoT architecture must be flexible to changes that the network encounters.
3) Interoperability: Heterogeneity is a prime characteristic of IoT data. Well-defined standards and middleware are necessary to ensure ubiquitous computing.
4) Latency prevention: The data processing must be done in a timely manner, especially in critical application domains.
5) Accuracy: The data must be consistent and accurate throughout the process. The veracity of the data must be ensured, and the communication should be non-lossy.
6) Fault tolerance: The architecture must contain a distributed and decentralized system to ensure robustness and resilience.
7) Security protection: Data must be protected against malicious cyberattacks. The transmitted data must not be altered at any level.
8) Privacy Preservation: The transmitted data must only be available to the users participating in exchanging information.
9) Low cost: The overall cost of deployment, network communication, storage, and maintenance should be low. Affordability is an essential factor in making IoT a viable business paradigm.
10) Scalability: IoT is an ever-growing field. New devices are added to expand the existing networks. The architecture must be flexible to the growth of the network

1) *IoT Security Goals*

An IoT network must satisfy the following security goals:

1) Confidentiality: Data transmitted must be accessible only to authentic users. Encryption mechanisms must be employed to protect the data.
2) Integrity: The data transmitted must be trustworthy. The data received must not be modified in an unauthorized manner.
3) Availability: The data must not be lost in transit. DoS must be avoided.
4) Authenticity: The data must originate only from trusted sources only. The Authentication issue includes the capability to identify the devices in the IoT-based system.
5) Non-Repudiation: The data transfer must be bound by proof of data ownership. The sender and receiver must acknowledge the transfer of data and not deny it at a later stage.
6) Authorization: This refers to granting permissions to access data or perform an operation on authenticated objects and persons.

B. *Security of Centralized IoT applications:*

The number of IoT applications has increased significantly as a result ofthe development of open-source cloud platforms, such as Azure IoT Suite, Amazon Web Services, and Oracle IoT. IoT is at the root of various critical application infrastructures such as Smart Home, Smart City, Smart Health, Smart Agriculture, Smart Retails, Supply Chain Management, Finance, Industrial Control Systems, Communication Networks, Smart Grids, and Smart Transportation [7]. These applications generate personal and sensitive information, raising the need for secure DM. Centralized schemes are susceptible to attacks, and a hacker can modify the AC policies to gain control of the system. Decentralized schemes are necessary for securing IoT Applications. The centralized nature of the application is vulnerable to various security threats at all levels, as depicted in Figure 2. In this subsection, we discuss six critical application domains:

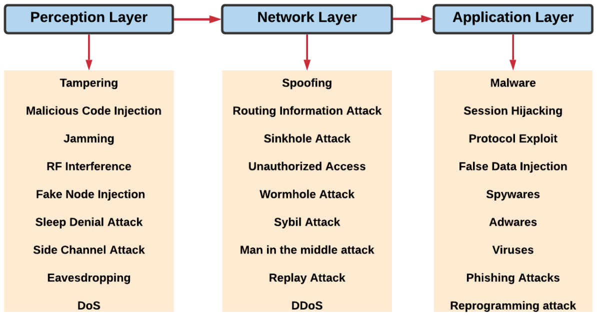


Figure 2. Security attacks in IoT

1) **Smart city (SCT):** SCT has Information and Communication Technology (ICT) at the core of its infrastructure. SCT provides several innovative and advanced services to its citizens to improve their quality of life. Intelligent information is provided to its citizens in real-time by fully enabling the control of the physical objects. Various SCT applications include Healthcare, Smart buildings, Public safety, Smart Governance, and Smart agriculture. SCT faces large-scale security and privacy risks. The resource-constrained devices used, such as sensors and cameras which collect and share sensitive information, are very vulnerable to attacks by hackers. Most of the resource-constrained devices have no adequate security or privacy mechanism. The communication technologies used by IoT devices like RFID, NFC, WiFi, LPWAN (Low Power Wide-area-network), 6LoWPAN 3G,and 4G mobile technologies are highly susceptible to attacks. The presence of multiple links between many system components exposes them to many security risks [8], [9], [10].
2) **Smart HealthCare (SHC):** One of the major domains in the IoT-based infrastructure is SHC. Wearable and mobile devices in IoT-based SHC have added tremendous value to the healthcare domain. SHC is responsible for making healthcare personalized, more convenient, and efficient. The various applications of SHC include assisting diagnosis and treatment, health management, disease prevention, risk monitoring, virtual assistants, smart hospitals, and assisting drug research. SHC is highly vulnerable to security breaches and faces many malignant attacks, including privacy leakage, data tampering, and forgery. SHC deals with sensitive and personal data. The data collected through sensors are both static or have dynamic behavior. The breach of such data is considered a severe breach in data protection. The connected devices capture, aggregate, process, and then transfer the data to the cloud. These devices are vulnerable to tag cloning, spoofing, RF Jamming, and cloud polling. SHC has a centralized dataset that contains personal information such as family history, electronic medical records, and genomic data that must be secured from malicious software. Wireless networking technology deployed in the healthcare environment like Wi-Fi, BLE, and ZigBee results in an increased threat of eavesdropping, sybil, and sinkhole attacks [11], [12], [13].
3) **Smart Grid (SG):** SG constitutes one of the most critical applications of the IoT. SG entails integrating the data communications network and the power grid to analyze the data collected from transmission lines, distribution substations, and consumers. The transmission and distribution of the power networks in SG are intelligently monitored at a fine granularity for high accuracy. Several IoT architectures have been proposed to be integrated with SG. Layer 1 architecture consists of the Smart meters, Network Devices, and Communication protocol in the general three-layered architecture. Layer 2 contains devices responsible for receiving data at the central system. Layer 3 includes artificial intelligent systems to provide information to decision and billing systems. IoT-based SG as a cyber system faces security challenges at all three levels. The attacks can be categorized into four main types: Device attack, Data attack, Privacy attack, and Network availability attack. Authentication, user privacy, and data integrity are essential in SG. Only the intended recipients must access the data stored or transmitted. Secure authorization and control access is an important issue for IoT-based SG. Only a certified and authorized person should be granted the necessary access to perform any configuration of the smart meter [14], [15], [16].
4) **Smart Home (SH):** An IoT-based SH refers to the environment of living that consists of highly intelligent and advanced automatic systems. Smart services are provided by various heterogeneous electronic devices networked together to provide smart services. An IoT-based SH performs various functionalities such as controlling and monitoring lighting, home temperature, appliances, intrusion detection, and energy management. Convenience and security are considered two key factors influencing the decision of the users in adopting IoT-based SHs. An SH must satisfy five security goals- Authentication, Authorization, Integrity, Confidentiality, and Availability. SH faces many security-related issues owing to its basic architecture, such as eavesdropping. An attacker can capture the traffic in infrastructure among the different components of SH, thus violating confidentiality. The data captured can lead to an impersonation attack where an adversary masquerades as an authentic user and accesses IoT resources. DoS attacks can be performed by crafting malformed messages, resulting in provided service not processing the data properly, thereby compromising the availability [17], [18], [19].
5) **Smart Farming/Agriculture (SF/SA):** IoT-based SF solutions refer to the system in which the crop field is monitored with the help of sensors, and the irrigation system is automated. The monitoring of the farm can be done from anywhere by the farmer. In IoT Smart Agriculture (SA), far advanced sensors are utilized, connected to the cloud via cellular and satellite networks. Thus the real-time data received assists in making effective decisions. However, there remain many security and privacy issues which are critical to the performance of SA/SF. Wireless sensors are used abundantly in SA to give up-to-date information to the farmer in real-time. Centralized systems store the information and have control over it, compromising the privacy of the system. Furthermore, communication plays a key role in SA/SF. The vulnerable nature of wireless

technology results in the interception of data packets. The data is susceptible to modification while relaying them to their destinations, compromising the CIA triad and leading to incorrect decision-making [20], [21], [22].

6) **Smart Transportation:** With the rapid development in smart sensors, smart vehicles, and vehicular communication technology, the Internet of Vehicles (IoV) is proposed to be the future of the transportation critical infrastructure system. The evolution of the IoV can be considered from its parent branch of IoT, with the focus on Vehicular Adhoc Networks. With sensors embedded in the vehicles, mobile phones, and the devices installed in the city, there is a possibility to offer an optimized suggestion of routes, easy parking reservations, economic street lightning, prevention of accidents, and autonomous car driving. Due to the dynamic nature of the vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication, the real-time traffic state information measured and shared is essential in providing efficient and secure service in IoV. Since this communication is deployed in an open environment and topologies change over time, many vehicles enter the IoV system in a given time slot, making it challenging to identify and authenticate the legitimacy of each vehicle. This nature of the IoV network makes it difficult to ensure security and non-repudiation. As a result, the malicious attack can be easily launched to disrupt the services provided, leading to low traffic efficiency and compromising the safety of passengers. The high availability of IoV is important due to its safety-critical nature, which requires fail-safe, resilient, and fault-tolerant operations to be performed [23], [24], [25].

C. IoT Security Tasks:

The Security tasks can be broadly classified into five categories spanning different IoT infrastructure levels. These include:

1) Key and AC management: Only authorized personnel must be given access to perform an operation or to access data. Fine-grained AC mechanisms must be devised in a heterogeneous environment, where cross-domain interoperability is a must.
2) Authentication of Devices: It is a must that the legitimacy of every node participating in the network is proven to the root. The devices must also verify their data integrity and provide non-repudiation of the messages while interacting with other nodes.
3) Data sharing and Routing security: IoT system provides untethered access to information by transmitting data through uncertain and insecure channels. Securing the data and routing operation from cyber-attacks during transit is essential.
4) Prevention against software failures: IoT systems are susceptible to Malware threats that can disrupt the entire functionality of the system. Adware, Ransomware, Spyware protection is necessary to protect the IoT ecosystem.
5) Secure and privacy-preserving data storage and management: A central authority controls a centralized system that has complete control over the users' data. IoT systems require secure, tamper-resistant, and privacy-preserving database storage and management.

4. Blockchain Technology

Blockchain is a distributed digital ledger consisting of a series of time-stamped blocks linked together through a CM forming a decentralized and distributed network [26]. A set of rules guides the transactions, and the system is free of any central authority. Instead, a peer-peer (p2p) network is responsible for maintaining and updating the ledger. Conceived originally to prevent the "double-spending" problem in commercial transactions, the first widespread application of BC was the cryptocurrency Bitcoin'. However, since its inception in 2008, BCT has found applications in various other sectors such as Banking, Asset Management, Healthcare, IoT security, Identity management, and Insurance [27]. The World Economic Forum estimates that the BC would store 10 % of global GDP in the coming decade.

Blockchain is a decentralized ledger that contains transactional records.The information that is contained in the ledger is in digital format. A large number of transactions are contained in the block of the BC.For every transaction that occurs in the BC, the author's digital signature is required, and every participant's ledger is updated.By the very inherent design of the BC,the chain's data is highly secure, which guarantees the fidelity and security of a record of the data.This generates trust without the need for some other third party. The validation and tamper-resistant transactions are managed by a large number of nodes[28].BC can also be described as distributed ledger technology that provides certificates to prove that information has not been tampered with[29].

Four crucial technologies are guiding BCT. These include Hashing, Cryptography, Digital signatures, and Consensus. Hash function takes data of indefinite sizes as input and gives a value of definite size in the output. Even a minor change in the input leads to a completely different hash value. BCT is based on the SHA-256 hash function.The corresponding hash is computed in the encryption block when a transaction is made, and the blocks are connected through the hashes [30]. For secure interaction, BCT employs public-key asymmetric cryptography [31]. Cryptography ensures confidentiality, accessibility, and integrity,assuming that the attack is computationally bound (the probability of which is high). Membership services governed by protocols maintain and manage the unique chain identity of the user. BCT uses a public key –private key mechanism for the identification of devices and signing transactions. A wallet contains information about public and private keys and tokenized digital assets associated with the client. Every transaction on the chain is digitally signed, thus associated

TABLE I. Comparison of Blockchain types.

Characteristics	Permissionless	Permissioned	Consortium
Decentralization	High	Low	Moderate
Scalability	Low	High	Moderate
Immutability	High	Low	Moderate
Computational overheads	High	Low	Moderate
Communication overheads	High	Low	Moderate
Storage requirement	High	Low	Moderate
Power consumption	High	Low	Moderate
Latency	High	Low	Moderate
Openness	High	Low	Moderate

with the on-record identity of the client.The CM governs network synchronization in the open network and ensures that the system verifies any transaction initiated. These four technologies enable the following in BCT-based open-access systems: [32]

1) Decentralization: The transactions are validated without the interference of a central authority. The system is decentralized, and the information is distributed and replicated across multiple nodes. The nodes agree upon the actual state of the ledger through a CM.
2) Auditability: The records and transaction history on the chain serves as proof of ownership of the client's digital assets and the transactions associated with them. The historical timestamp associated with the data is permanently stored in the BC.
3) Integrity: The blocks are linked in chronological order with hashes. Thus, any malicious attempt to tamper with a block is readily detected.
4) Transparency: BCs impart trust in a trustless environment. A copy of the transaction information is visible to all the nodes. Any node can join an open BC system and access the network. The data is visible to everyone in the chain involved in the verification of transactions.
5) Immutability:A record, once written, takes up a permanent place in the ledger. The ledger holds these records perpetually, imparting verifiability in the system.

BCs are of 3 types- Public BCs, Private, and Consortium BCs. Public/ Permissionless BCs allow any user to join the network based on the consensus protocol, e.g., Bitcoin. Public BC has the capability of turning into a global network. A Private/Permissioned BC allows a specific set of nodes to be added to the chain providing a closed and more secure network [33]. Private BC is centrally controlled, and such a network is ideal for transmitting and sharing data within an organization. E.g., GemOS is a private BC. Finally, a hybrid approach that is partially centralized with lesser validators is called a consortium/Federated BC, where the control is distributed across a set of computers. Ethereum is a platform for building consortium BCs [34]. A comparison of the characteristics of the three types of BCs is depicted in Table I.

A. *Blockchain Framework:*

A Blockchain system has three layers- Data layer, Consensus Layer, and Application layer.

1) **Data Layer:** Data layer governs the block creation. Secure identities are provided to each node, and dependence is created through network protocols. The network protocols govern the formation of p2p networks and secure transmission over links. The blocks contain two prime components- Chain of blocks and Transaction array.
   a) Chain of Blocks: BC is a distributed database containing a sequence of blocks that stores records of value and interest. Each block has a Block header(BH) and a Block body(BB). The BH stores the block version, which specifies the block validation rule set, a nonce which acts as a counter to verify the hash, a timestamp to denote time, a Merkle root which stores the hash of all the underlying hashes of all the transactions in a cryptographic data structure called Merkle tree, the current block hash and the hash of the previous block. The BB contains the transaction data, an object recorded on blocks, organized by the Merkle tree [35].
   b) Transaction array: Every transaction is stored in the transaction array before adding it to the block. The transactions refer to exchanging value assets such as sending money, data, values, and messages. The basic skeleton of a Blockchain is shown in Figure 3.
2) **Consensus layer:**This layer performs the core functionality of a BC system, i.e., bringing agreement on the system state in a trustless environment through consensus. The consensus is generally achieved by choosing a miner who packs the transactions into a new block and broadcasts it to the network. Figure 4 shows the steps involved in BC-based transactions. The four most popular BC CMs are Proof of Work(PoW), Proof of stake(PoS), Delegated

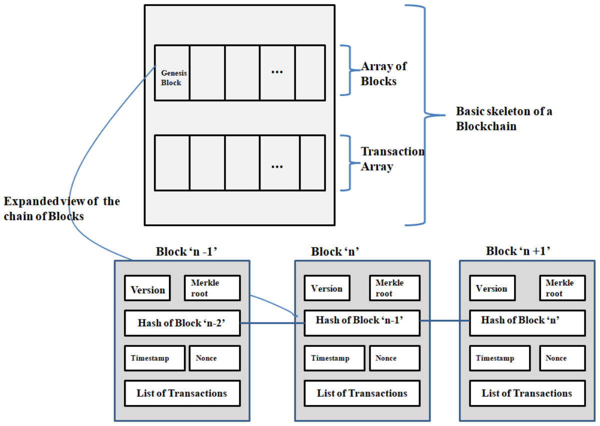
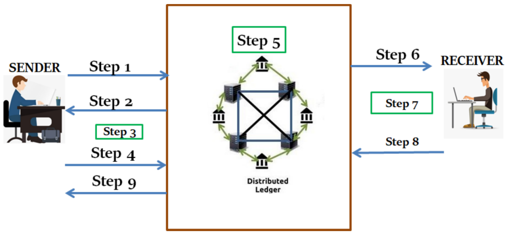


Figure 3. A basic skeleton of Blockchain.

Proof of stake(DPoS), and Practical Byzantine Fault Tolerance(PBFT). In PoW, the stakeholder(s)/miners compete to mine the block by calculating hashes until one node has the relevant value. In two nodes attaining the value simultaneously(rare) and the chain branches, the longest chain after the next block is taken as the real chain making the chains metastable. PoW requires complex computation and power resources. In PoS, a stakeholder/validator is chosen through a quasi-random process depending on his wallet credit, making the system run on low energy and computing resources but encouraging the nodes with nothing at stake to misbehave. In PBFT, the majority must agree on the network's state, i.e., for a client transaction to commit, 2/3rd of the network must validate it. In DPoS, the nodes /delegates are chosen through voting to add a block to the root chain. In case of abnormal behavior by the delegate node, the other nodes can vote it out. However, the delegates are significantly less than the network and govern consensus, encouraging centralization. Some more CMs are Proof of Delegated Byzantine Fault Tolerance(DBFT), Proof of Burn(PoB), Proof of Capacity(PoC), Proof of Elapsed time(PoET), Dirted Acyclic graphs(DAG), Proof of Activity(PoA), Proof of Importance(PoI), and Leased Proof of Stake(LPoS) [36].



Step 1: Sender broadcasts transaction "T1" to the network
Step 2:The network accepts the request and updates the ledger
Step 3: The sender computes the Digital Signature(DS).
Step 4: The sender broadcasts its DS to the network.
Step 5: Based on the consensus algorithm used, the peers in the network validate the transaction.
Step 6: The transaction is forwarded to the receiver.
Step7: The receiver uses the public paired key for decryption.
Step 8: The receiver sends an acknowledgement(ACK)message to the network.
Step 9: The network forwards the ACK to the sender.
Step 5 forPoW:
I) One miner broadcasts the transaction the network.
II) All miners compete by solvinga computational puzzle.
III) Fastest node matches thePoWand DS and broadcasts to all .
IV)All nodes verifyPoWwith DS ,the block is validated.
VI)The miner is rewarded and validated block is broadcasted to BC
VII)Theblock is added distributed ledger is updated
Step 5 II)Solving the puzzle
i) Network provides a difficulty rate
ii) Miner frames the header which has "Nonce"
iii) Miner computes Nonce
iv) Miner hashes the header using SHA256 function twice
vi) The calculated value becomes the current block hash

Figure 4. BC-based transactions.

3) **Application layer:** The Application layer provides interfaces for Distributed applications(DApps) that run on top of the BC system. At this level, SCs are integrated to guide the clauses' execution without human intervention. SCs are digitized versions of paper-based contracts that allow terms reliant on decentralized consensus by self-execution [37]. SCs are deterministic, autonomous, rule-based, and have unique addresses on the chain. The terms in the contract are converted into code that gets invoked automatically in case of contract violation. SCs identify frauds and malicious attempts in the system, thereby increasing security. The results are deterministic and have high accuracy. SCs are invoked independently and autonomously, mitigating the transaction costs by reducing human interference. Many BC communities are integrating interfaces for SCs, e.g., Ethereum provides a platform for writing SCs, written in a Turing complete language called Solidity [38].

5. Related Surveys:

IoT security is a vast domain, and many research and survey papers are available in the literature spanning various security aspects such as data encryption, intrusion detection, active attacks, passive attacks, device authentication, AC mechanisms, and channel security. AI and ML have complemented IoT security in recent times by providing improved real-time detection rates and attack detection accuracy. BC is a very recent addition to IoT security. BC addition to IoT is an up-and-coming solution to augment the pace of futuristic secure IoT networks. Due to the vastness of the domain and applicability beyond security, exhaustive survey papers are not available. Table II presents the recent (2019-2022) surveys available in the literature for BC-IoT integration. The surveys have been broadly classified into BC-based IoT Security, BC-based CMs for IoT, BC-IoT applications, BC-ML for IoT, and BC-EC integration. The focal points of each survey have been highlighted.

6. Blockchain as a key enabling technology in IoT

IoT is the focal point of enabling the pervasive interconnection of virtual and physical objects that have sped up data sharing and collection. This capability makes IoT one of the essential architectures for providing services in various fields. This section discusses BC as a key enabling technology for IoT and the technologies that drive BC and mitigate the challenges associated with BC adoption in IoT.

1) **Addition of BC features:** BCT offers unique characteristics such as auditing capability, traceability, immutability, interoperability, accessibility, and accountability, which are imparted in IoT systems with its adoption. The IoT data streams from diverse, heterogeneous environments are transformed into uniform coding. BC enables IoT and physical systems to collaborate through uniform access, facilitating cross-domain interactions [77]. BCs enable fine-grained access mechanisms and SCs to prevent unauthorized access making the systems open to interactions from other physical systems. Further, BC has a 160-bit address space higher than IPV6, aiding it to be more scalable. The IoT data is stored as transactions permanently in an immutable fashion on the network. Every transaction initiated by a node is associated with the corresponding information. Any misbehavior or fraud can be traced back to the user imparting the audit capacity in the system, which can highly complement IoT verticals [65].
2) **5G and 6G enabled Industrial IoT:** The advancements in faster communication networks are revolutionizing network services and making IoT systems faster. B5G technologies are key facilitators in innovating futuristic open access with low cross-domain barriers. The B5G systems need efficient communication mechanisms with enhanced security, robustness, privacy preservation, and improved mobility. 5Gs employ network slice brokers to enable mediation between vertical service and resource providers. BC can operate independently in slices enabling secure and anonymous transactions [4], [78]. 5G applications such as 5G-powered drones need security and enhanced privacy [79]. Various BC-based solutions have been presented for securing B5G and 6G systems. In [80], the authors present a BC sidechain-based decentralized hierarchical scheme for 5G to provide secure communication and authentication. The authentication is done at the edge of the network to reduce latency. In [81], the authors propose a BC-enabled clustered architecture for validating blocks in IoTs for B5G applications.
3) **Enhanced automation with SC applicability:** With the help of SCs, BC is imparted with decision-making capabilities that drastically reduce human effort, and the applicability of IoT systems is increased [82]. The transactional clauses of SCs are digitized and tamper-resistant and cannot be modified. SCs eliminate the need for an intermediator, minimizing management costs. SCs detect breaches and misbehavior in the system and automatically take decisions depending on the clauses pre-agreed upon by the system's stakeholders. The decisions have higher accuracy and reliability and improve the overall security and efficiency of the system. SCs make distributed access decisions to enable legitimate users to query the BC and work better with data-driven interactions. SCs are deterministic and autonomous, thereby accelerating the inception of Decentralized Autonomous Organizations(DAOs). In IoT systems, SCs facilitate flexible AC, secure DM, prevent DDoS attacks, and provide secure identity management, strengthening security further.

The three primary driving forces for BC-IoT adoption are:

1) **Edge computing:** EC is a major driver for IIoT, and the integration of BCT into edge provides enhanced reliability, privacy, data integrity, reliable AC, and automated resource allocation. Conversely, the edge networks provide computational, storage, and side chain-based consensus facilities to IoT devices [70]. Due to the constrained nature of IoT end-devices, they communicate data to the edge where the moderately intensive CMs and functions are done. The nodes store partial data such as time-stamp information to validate the authenticity of the other nodes. At the same time, the complex functions, strong CMs, and high storage requirements are offloaded to the edge. Various architectures have been present for BC-based edge computing. In [83], the authors propose a mobile BC-assisted IoT application consisting of Small cell base stations with mobile edge computing (MEC) deployed at them. In [84], the authors present a prototype for BC-based EC for mining and edge resource management for mobile BC. In [85], the authors present a DPoS based double auction cross-server edge resource allocation framework for mobile EC. BC functionality can be further extended for network management by designing BC-based Software-defined networks [32].
2) **Integration with ML:** BCs provide secure data storage, and the outputs can detect anomalies in IoT systems [86]. The integration of ML and BCT in IoT can enable various tasks such as - secure storage of correct data, monetization of ML skill set through SCs, feeding correct data into algorithms, creation of better learning models through incentive-based competitive modeling, Making BCs secure from attacks, enabling automated signing of BC systems [71], [87], [88], [89]. In [90], the authors proposed a BC-assisted collective learning method to guide the secure exchange of learning results at the IoT edge. The model employs BC on the top of the edge devices where the nodes securely share learning results using BC-assisted collective

TABLE II. Related Surveys

Focal Point	Reference	Year	Key Highlight(s) of the Survey
General Surveys with Key focus on Security.	[39]	2022	• Distributed Denial of Services(DDoS) attacks • BC- based solutions to mitigate DDoS attacks
	[40]	2022	• BC taxonomy for IoT applications. • Blockchain platforms for IoT.
	[41]	2022	• BC for big data- Services • BC –based big data projects
	[42]	2021	• Architecture of SCs. • Levels of BC-IoT Integration • BC-based IoT applications
	[43]	2021	• Layer-wise security threats in IoT • BC security solutions for IoT
	[44]	2021	• Potential of SC integration in IoT • Decentralized architecture for BC-based IoT systems
	[45]	2021	• BC-based AC methods for IoT • BC-based IoT use cases
	[46]	2020	• Need for continuous authentication schemes in IoT • BC-based security solutions
	[47]	2020	• IoT trust management system • BC-based trust management system.
	[48]	2020	• Layer-wise security attacks in Industrial IoT (IIoT). • BC addition to IIoT.
	[49]	2019	• Security concerns underlying IoT communication protocols. • BC-based cybersecurity in IoT
	[50]	2020	• Primary study of BC-based cybersecurity of papers until early 2018
	[51]	2019	• Attacks against CMs • BC extensions
	[52]	2019	• Schemes for BC-IoT integration • BC-based IoT Privacy
Consensus Algorithms	[53]	2020	• Comparison of BC-based CMs and their suitability for IoT.
	[54]	2020	• Evaluation of CMs on four criteria -Throughput, profitability, decentralization degree, and security.
	[55]	2020	• Discussion on various BC architectures and protocols. • Consensus characteristic in BC-based IoT applications.
	[56]	2020	• Discussion on CMs and their division into four groups based on scalability, security, energy consumption, and throughput.
	[57]	2020	• Review of BCT implementation in IoT concerning CMs. • Frameworks for IoT-BC implementation.
	[6]	2020	• Limitations of PoW and PoS for IoT. • Distributed consensus. • Directed Acyclic graphs based consensus methods and challenges.
	[58]	2020	• A comprehensive review of the suitability of CMs in IoT. • Frameworks for BC implementation.
Blockchain-based IoT Applications	[59]	2020	• BC-based Applications for CPS • Evaluation of BC-based improvement in IoT applications.
	[60]	2020	• BC IoT Projects • BC-IoT Use cases
	[61]	2019	• Applicability of BCT for Smart communities- Finance, ITS, SG, SHC, and Voting systems. • BCs in Process models

	[21]	2020	• The architecture of Green-IoT-based agriculture and threat Models. • BC-based Security solutions and challenges.
	[62]	2020	• BC integration in 5G enabled UAV networks. • Network security challenges in UAV.
	[63]	2020	• Attack models in Precision Irrigation (PI) systems. • BC integration in PI to mitigate Attacks.
	[64]	2020	• BC as a Solution for smart applications in precision agriculture. • BC platforms in precision agriculture
	[65]	2020	• Review of BC-based Supply Chain.
	[66]	2021	• BC-based IoT use cases for SHC. • A comparison of CMs for healthcare applications.
	[67]	2021	• BC applications in smart environments in smart cities and challenges. • Data-centric requirements for BC-based smart cities.
	[68]	2021	• BC application in IoV for ITS. • BC-based IoV architectures. • Benefits and limitations in BC-based IoV
Blockchain for B5G applications and integration with ML	[32]	2019	• BC deployment in IoT and applications. • BC for B5G-IoT
	[69]	2020	• BC and 5G enabled IoT applications.
	[70]	2019	• Secure Edge Intelligent BC-powered B5G networks. • Optimal resource scheduling using a deep reinforcement learning approach.
	[71]	2020	• Convergence of ML in BC-based IoT Applications- Benefits and challenges.
	[72]	2020	• ML and BC Integration for IoT. • BC security mechanisms for IoT.
Blockchain-Cloud-Edge Computing	[73]	2020	• Comparative analysis of Cloud-based IoT Vs BC-Based IoT.
	[74]	2019	• BC –Software-defined network integration and frameworks.
	[75]	2019	• Security Challenges In Fog computing • BC as a security solution for Fog Enabled IoT Systems
	[76]	2020	• Motivation for integrating BC with Cloud of Things (CoT). • Architecture and applications of BC integrated CoT

learning. The authors propose a modified Proof of Learning consensus algorithm where work is done in the training process instead of solving a random puzzle. The learning results from the winner are adopted in the rest of the deep neural networks.

3) **IPFS powered BC for IoT:** In critical IoT systems, distributing data in a tamper-proof and traceable manner is necessary. BCs provide the service, but they work inefficiently while handling big data considering the transactional processing limitations. IPFS can complement BC and provide a secure storage mechanism for IoT data. IPFS is a content-addressable, p2p version-controlled file system that can assist the formation of a decentralized IoT system [91]. IPFS, based on cryptographic hashes, is a potential alternative to address BC big data issues. BC is duplicated on multiple nodes; thus, most storage spaces are required without immediate use, particularly if the node operator does not need to examine every file saved on BC. With IPFS, BC only saves the cryptographic hashes slowing down the chain development drastically because hashes are typically less than the data they represent. For example, if SHA256 is employed, the on-chain storage required for a file of any size is lowered to 32 bytes [92]. For any modifications in the content, the hash value changes each time. The authors of [93] offer a decentralized IIoT data management system

based on BC and IPFS. The authors of [94] propose a network architecture that uses BCand IPFS to provide IoT data privacy. SCs perform AC in the proposed “modular consortium” architecture while also providing accountability for data owners and third parties to whom users grant access.

7. Blockchain Integrated IoT systems.

IoT aims to design a distributed system offering scalability, security, privacy, reliability, real-time data delivery, and high adaptability. With the rapid advancements in B5G, IoT systems are becoming faster, expanding over longer ranges, and requiring enhanced security solutions. BC has distinguished intrinsic features of non-intermediation, immutability, data transparency, and tamper-resilience, which mitigate security concerns in an untrusted cross-domain open environment. BCs are envisioned as the future of open-access systems requiring distributed storage, efficient data and resource management, secure KM, and AC mechanisms. By design, a BC-based architecture can ensure confidentiality, integrity, availability, user control, and authorization in any system [95]. The integration of BC into IoT offers increased data trust, imparts verifiability, eliminates intermediation, provides transparency, and increases user control of the user data in the systems. IoT and BC’s collaboration can resolve the issues of data organization, data maintenance, communication security, intra-domain collaboration, and privacy in IoT. We shall refer to such systems as BC integrated IoT (BIIT) systems throughout the rest of the paper.

A. Technicalities of Blockchain IoT integration:

The world is moving towards becoming “smart” with IoT technology, necessitating more attention to data security and privacy concerns. IoT security solutions are typically complicated due to a lack of safe hardware and software design, development, limited resources, and established standards. Furthermore, the diversity of resources available in the IoT has hampered efforts to develop a comprehensive global strategy for protecting IoT systems at all levels. The main challenge is data management and securely providing services without compromising the privacy of the underlying personal information. One of the IoT security solutions is to develop a fine-tuned AC mechanism for data protection and privacy by ensuring that only authorized and authenticated users may access data. However, this is hindered by the vastness of the connected devices. Furthermore, the traffic created by the massive amount of data generated by these devices makes satisfying quality-of-service standards difficult. loT devices have low storage, computation power, and bandwidth restrictions.

With all of the interactions between people, data, and devices, IoT promises direct connectivity between devices and data interchange. In the IoT economy, sensors and devices should be able to conduct monetary transactions in exchange for services without the involvement of a third party. With the introduction of the 5G network, transactions and exchanges will predominantly occur over the internet network, which billing and payment systems must account for. However, financial institutions can still not receive real-time information on pledged assets due to ineffective management for accessing, sharing, and analyzing asset information across stakeholders. There are no chattel asset tracking and monitoring systems capable of validating and quantifying chattel assets pledged for loans.

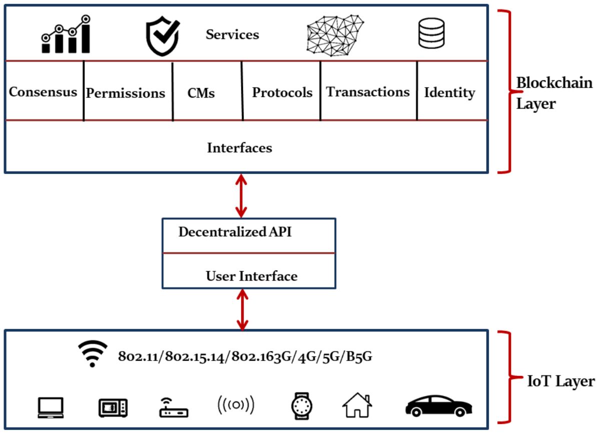


Figure 5. Interaction between IoT and Blockchain

BCT has the capability of bringing reforms in these sectors as it enables safe, immutable, and anonymous transactions using a decentralized distributed ledger system. BC-enabled loT systems can monitor and track chattel assets in transit or warehouses in real-time. The combined approach aids in the resolution and avoidance of unnecessary risks in the financial industry. Some attacks on loT systems can be addressed using BCT. BC research as a security mechanism has resulted in various transformative benefits that were previously unattainable or unavailable. Figure 5 depicts the interaction between IoT devices and BC platforms.

Figure 6 illustrates a simple BC-based security level evaluation mechanism for IoT. The authors of [96] illustrate the steps involved in an IoT network based on BC. First, IoT device manufacturers pre-verify software that is loaded on IoT devices and create the whitelist. A SC is produced by combining a manufacturer’s whitelist and the agent’s initial agent hash value(IAHV) installed in an IoT device. IoT device manufacturers can access SCs via decentralized applications or internally through an Application Programming Interface(API). IoT device manufacturers use SCs to update the White List. Manufacturers use the whitelist SC to record the whitelist and IAHV of the agent installed in an IoT device in the BC. By inquiring about the information recorded in the BC via the whitelist SC, the IoT device can verify that the agent’s IAHV matches the device agent hash value of the installed agent. It validates that the agent has not been forged or fabricated by comparing it to the agent hash value stored in the BC; as a result, the security evaluation process of IoT devices via the agent may be trusted. The IoT device’s agent checks to see whether any

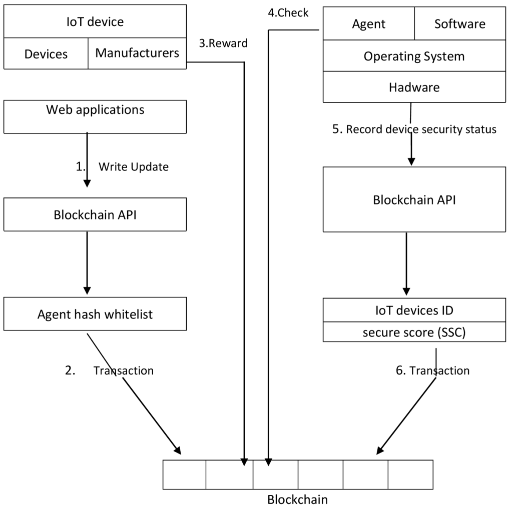


Figure 6. A simple BC-based security level evaluation mechanism for IoT.

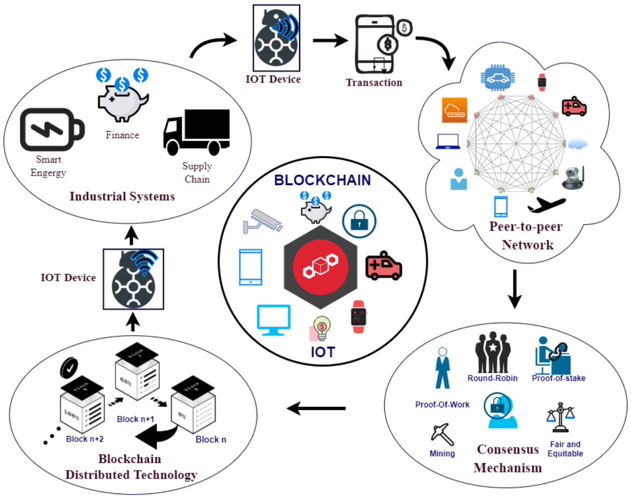


Figure 7. Overview of Blockchain –based IoT architecture

untrusted programs have been installed. The agent evaluates the security status of the IoT device and transmits it to the scoring SC. Manufacturers receive rewards in return for updating the whitelist SC.

1) Recent proposed architectures:

Two main features of the BCT include Trust and Decentralization [97], [98], [99]. By design, the data on a BC is secure and tamper-resistant, making it a key disruptor for IoT. BCs can be utilized to improve IoT in the following ways:

1) Impart data integrity: The nodes in the BC have identical copies of the ledger. When transactions occur, all network members are responsible for validating them, and once verified and stored in the ledger, the transaction cannot be manipulated or removed.
2) More Addressing space than IPV6: BC addresses are 160 bits long, while IPV6 addresses are 128 bits. When compared to IPV6, BC has higher addressing space (4.3 billion addresses).
3) Trusted accountability: Every operation is documented in the ledger; thus, it is possible to identify and trace all operations.
4) Fault tolerance: Decentralized systems rely on multiple separate components; they are more fault-tolerant. Because of the point-to-point decentralized structure, BC has no single node failure concern.
5) Eliminating third-party liabilities: BC runs without third-party intermediaries and is free of any risks or dangers posed by third parties.

The decentralized. peer-to-peer architecture is the most notable characteristic of BCT. The distributed ledger contains all transactions, and all network members must agree to approve the transaction. This feature enables the implementation of end-to-end traceability. Data provenance was previously difficult to obtain, but it is now a possibility with the BCT's distributed ledger option. Owing to these benefits, many BC-based architectures have been proposed for IoT; an overview of the same is provided in Figure 7. The authors of [100] propose the solutions to overcome the centralized solutions and security measures in IoT. The data-driven decentralized mechanism is used, which provides energy-efficient solutions for detecting attacks on the IoT-based Sensor Networks. In [101], the authors aim to facilitate the data searching and extraction of public and private BCs deployed at the MEC server of the 5G MEC smart grid. IoT device identifier is built as a BC explorer. In [102], the vulnerability of the massive data produced in IoT networks for smart transportation is solved by the BC and IoT, which provide a decentralized data management system. In [103], the authors propose using the Identity Based Encryption (IBE) algorithm to enhance health care data security.The BC-based IoT architecture uses IBE to provide enhanced security. In [104], the authors address the privacy, security, and scalability issues in a centralized system for IoT and resolve them with a lightweight architecture for BC-based identity management. In [105], Mobile edge-cloud computation offloading is used in delay-sensitive IoT applications. An effective, trustworthy access control mechanism is introduced, which involves an advanced deep reinforcement learning algorithm using a double dueling Q-network. The work in [106] proposed using BC, SCs, and IoT devices to integrate different kinds of IoT devices in pre and post-harvesting agriculture segments. This work in [107] proposes the integration of the Software-Defined Network with the BC system. A BC-based architecture is used for proposing the new routing protocol witty cluster structure for the IoT networks.

B. Tradeoffs in Consensus mechanisms for IoT suitability BIIT systems:

Consensus is the principal mechanism that makes the BCs secure by design. A CM governs the rules that pivot on the network's nodes to agree on the ledger's true state. Consensus achieves trust in a heterogeneous, uncontrolled environment by providing a mechanism to validate the data communicated by the nodes in the network. CMs eliminate the central authority, validate the data communicated by the nodes in the network, establish trust among nodes and ensure a system state agreed upon by the network members. With the increase in BC-based applications, various CMs have been proposed and adopted by systems, but their adoption is met with challenges. The choice of the consensus algorithm significantly affects the network's performance, and there exists a tradeoff between scalability, energy consumption, bandwidth requirement, network overheads, computation overheads, security, privacy, and latency.

The robustness of a BC-based system is highly dependent on its underlying CM. The security provided by a CM is directly proportional to computational and bandwidth requirements, as is the case with PoW. IoT's computational and communication abilities are bound by constrained resources; thus, applying a generic CM in IoT is difficult. Inter-domain cross consensus poses additional challenges [108]. Over the past few years, CMs have been customized particularly for LW environments. Since IoT networks are constrained, the CMs have been modified over the last few years to increase their suitability in LW networks. This, however, comes at the cost of compromising security and other factors. CMs with strong fault tolerance and immunity to attacks require the computation of intensive hash operations that consume energy, bandwidth, and other resources. CMs that work on low power do so at the cost of decreasing the network's size or moderately compromising data integrity. An ideal CM for IoT would ensure increased decentralization, adversity tolerance, scalability, throughput, and decreased latency, energy consumption, storage, computation, and network overheads.

A comparative study of the existing CMs in light of IoT goals is presented in Table III [109], [58], [55], [53] and [60]. The values High, Moderate, and Low under different columns(to different methods) are assigned based on different criteria. For the energy consumption, computational resource requirements, storage overheads, and Throughput, the values are assigned bydirect comparison with PoW and IoT suitability. The numerical criteria for assigning latency values is Block creation time. For example, the block creation time in PoW is approximately 10 minutes, while it is only 4 minutes in PoC. Although the time is considerably lower than PoW, it is still not suitable for real-time IoT environments, and compared to other CMs that take only seconds, the time taken by PoC is high. Thus, the value "Moderate" has been assigned based on the combined criteria. DPoS can process 100,000 TPS, and the block is added in under 3 seconds to the chain, which is still not suitable for real-time IoT systems that require a block creation time of the order of milliseconds.

While designing a new consensus algorithm for an LW system, the following tradeoffs need to be considered:

1) Security and Computational requirements: Strong cryptographic methods provide high security and decentralization to the system, and improve data integrity and confidentiality but are computationally intensive and require high power systems for implementation.
2) Privacy and Latency: To achieve privacy, the adopted system should be free of a central authority, and the consensus should be achieved in a p2p fashion. However, private chains are adopted by systems that encourage centralization to decrease the system's latency, thereby increasing privacy concerns.
3) Convergence rate and Adversity tolerance: The convergence of the algorithm affects the adversity tolerance of the network. For IoT real-time systems, for the consensus to converge faster, the number of nodes involved in consensus is decreased, making it easy to compromise the network and decreasing the system's fault tolerance.
4) Latency and Scalability: For cross-domain access, the number of validations to perform transactions increases, increasing the network overhead. To reduce latency in real-time applications, the number of the communicating nodes needs to be capped.
5) Throughput and Scalability: As the network size increases, simultaneous communication attempts to access resources and Block addition increase considerably. This affects the system's throughput significantly as more nodes access the limited resources of the system

1) BIIT suitable Consensus mechanisms and Blockchain platforms:

1) **Hyperlegder Fabric with PBFT:** Hyperledger fabric has a modular architecture and can create private chains. The system's latency is less but is associated with significant network overhead, suitable for small private networks, limiting the network's scalability. Hyperledger fabric is suited for private networks, works on PBFT, and has a pluggable CM. To achieve consensus, the majority of the nodes must agree on the block addition. For writing SCs, the framework supports the "Go" language and "Chaincode" [135]. The framework provides data confidentiality, efficient processing, and identity management and is suitable for low-scale IoT implementation.
2) **Hyperledger Sawtooth with PoET:** Designed by Intel, this framework is suitable for low-powered systems. The nodes solve a hash problem, and the winning node is chosen randomly on a random waiting time using Intel's softguard extension. The contracts on Sawtooth can be written in any language, and various CMs can be plugged into the same chain [136]. It usually employs PoET, which offers low computational requirements, High

TABLE III. Comparison of Consensus mechanisms for IoT suitability.

Algo	NA	IoT goals							
		ECP	CRR	SO	CVG	STY	LTY	TPT	DEC/SEC
PoW [110]	PL	High	High	High	Very Slow	High	Very High	Low	Fully decentralized. Secure.
PoS [111]	PL	MDR	MDR	High	MDR	Fair	MDR	Low	Lower decentralization than PoW. Relatively lower tamper resistance to attacks.
PBFT [112]	PD	Low	Low	High	Fast	Low	Low	High	Low Decentralization. Prone to Sybil attacks.
DPoS [113]	PD	MDR	MDR	High	Fast	MDR	Low	High	Encourages centralization. Prone to attacks.
DBFT [114]	PD	Low	Low	High	MDR	MDR	MDR	High	MDR decentralization. Prone to security attacks.
PoC [115]	PL	Low	Low	Very High	MDR	High	MDR	High	Relatively high decentralization. Selfish mining.
PoET [116]	PD	MDR	Low	High	Fast	High	Low	High	Intel-Central authority Not truly decentralized.
LPoS [117]	PL	MDR	MDR	High	MDR	High	MDR	Low	Decentralized. Secure
PoA [118]	PL	High	High	High	MDR	High	MDR	Low	Decentralized Trust requirement.
PoI [119]	PL	MDR	MDR	High	MDR	High	MDR	High	High Decentralization. Takes into account nodes' reputation.
DAG [120]	PD	MDR	MDR	High	MDR	High	MDR	High	Susceptible to Sybil attacks.
Casper [121]	PL	MDR	MDR	High	MDR	High	MDR	MDR	Decentralized and secure.
Stellar [122]	PL	MDR	MDR	High	MDR	High	MDR	High	Decentralized. Robustness is achieved through quorum slices.
Ripple [123]	PL	Low	MDR	High	MDR	High	MDR	High	Decentralized. Can tolerate up to 20% faulty nodes.
Tendermint [124]	PD	MDR	MDR	High	Fast	High	Low	High	Not fully decentralized. Based on monetary concepts, which is not suitable for IoT
Rapid Chain [125]	PL	MDR	MDR	Low	MDR	High	MDR	High	Decentralized. Provides full sharding.
Omni Ledger [126]	PL	MDR	MDR	Low	MDR	Fair	MDR	High	Decentralized. Low Security. Can tolerate up to ¼ faulty nodes.
Elastico [127]	PL	High	High	High	MDR	High	High	Low	Decentralized. Suffers from Security risks.
RScoin [128]	PD	MDR	MDR	High	Fast	High	Low	High	Low Decentralization and based on monetary benefits.
Algorand [129]	PL	MDR	MDR	High	MDR	High	MDR	MDR	Decentralized and high security.
ByzCoin [130]	PL	High	High	High	MDR	Fair	MDR	High	Decentralized. Susceptible to DoS attacks.

PaXoS [131]	PD	Low	MDR	High	Slow	Fair	High	MDR	Decentralized. Fault-tolerant consensus among a group of nodes.
Tangle [132]	PL	Low	Low	Low	Fast	High	Low	High	Not fully decentralized. Security compromised if node gains > 1/3rd of hashes.
RAFT [133]	PD	MDR	MDR	High	Fast	MDR	Low	High	Not fully decentralized. Susceptible to ledger node failure.
Treechain [134]	PL/ PD	MDR	MDR	MDR	Fast	Fair	Low	High	Secure at the cost of overheads.

* NA, ECP, CRR, SO, CVG, SCY, LTY, TPT, DEC/SEC, MDR, PL, PD respectively stand for Network Access, Energy Consumption, Computational resource Requirement. Storage Overheads, Convergence, Scalability, Latency,Throughput, Decentralization/Security, Moderate, Permissionless, Permissioned.

throughput, and Low latency but encourages centralization. Hyper ledger Sawtooth platform is suitable for permissioned and permissionless BCs and provides features such as live data streams suited for IoT environments. The framework, however, suffers from Security and Privacy issues.

3) **IoTa with Tangle:** Tangle is a distributed communication protocol that does not work on transaction fees suitable for IoT. Tangle enables a parallel transaction verification mechanism which decreases the convergence time and reduces latency in the system. However, the framework suffers from storage and security problems and is prone to centralization. IoTa uses DAG, which minimizes the system's network and transaction overhead [132]. The latency is low and has been specifically designed for IoT applications. Iota enables high throughput but does not support SCs and suffers from privacy issues.

C. Security architecture of BIIT systems

BCT is evolving as a key paradigm in addressing these issues of IoT. In BIIT systems, BC is added at the security level and works on a distributed consensus scheme where each IoT transaction is verified, and every message can be traced to the origin. BIIT systems work in a p2p distributed manner, and each entry is time-stamped. The data blocks are integrated using cryptographic hashes, and the Merkle tree stores all atomic transactions. The tree's root hash is verified to secure all the transactions underlying it.

To understand the BIIT system's security mechanism, the Hyperledger fabric for IoT BC security architecture has been considered, consisting of five levels: [137]

1) Perception layer: The IoT node layer collects the data from heterogeneous environments and is pre-processed, transformed, and stored on BCs.
2) Network Layer: All nodes are given equal priority and transmit the data. Each node contains the data authentication protocol information and block network mode.
3) Consensus layer: The layer works on the PBFT algorithm, suitable for constrained IoT environments because of less energy consumption and lower computational overhead.
4) Smart Contract Layer: The SC layer stores contracts, incentive mechanisms, and other scripts. SCs are set up in the certification authority.
5) Application Layer: The layer is responsible for collecting, storing, verifying, and processing the data blocks. The IoT application interface enforces the node transaction process and provides AC services.

Mechanism: The devices are registered and granted AC rights which are defined in the SC. Various sensing devices collect data of various types and in varying formats. This data is pre-processed, and preliminary information is extracted through a hash function and asymmetric encryption. The heterogeneity is removed by transforming the data into a fixed-length base to keep a uniform format. The data is time-stamped, stored in a block, and broadcasted to the whole network. The gateway nodes hash the data, storing the table in the block. The time-stamp archives the key block information such as the source, and digital signature, which imparts traceability. Any node can act as a miner to carry out authentication. A block node validates the received data according to the data structure, source, time-stamp, and other information. The data from a legitimate source is added in chronological order, and the transmission from a malicious node is restricted. The data is stored in an immutable fashion on the chain.The IoT transactions are verified using a PBFT consensus algorithm, ensuring that no false data is stored on the system. The SCs are triggered in case of an event, and the contract clauses are invoked to handle the misbehavior by one or more nodes. SCs enable cross-domain interoperability by implementing scripts for various states. The SCs also eliminate human/third-party intervention for invoking the rules in case of a malicious attempt. At the top, application services are provided, and access rules for cross-domain interactions are maintained. The architecture has five prime advantages-Improved security, increased cross-domain interoperability, data integrity, data traceability, and automated decision making.

8. BIIT systems and IoT Security tasks

More and more devices are being connected in the IoT application domains with advancements in sensing and actuating technologies. Verifying the legitimacy of the components for secure communication, authentication schemes, and secure routing protocols (RP) are essential criteria in IoT sensor networking. In Table IV, the literature study of the recently proposed security architectures of BIIT systems has been summarized vis-à-vis security tasks identified in Section 3.3.

A. *Primary Study of the BC Solutions:*

In [138], the authors propose a BC-based distributed KM scalable architecture with fine-grained auditing capability for hierarchical AC. The architecture consists of 3 main components- A device layer containing the CPS devices, a BCT-based security access manager (SAM) network at the fog layer, and multiple BC networks on the cloud for KM. The user keys are secured and not under the control of a key generation center, and the information is instead stored on the SAMs, which act as the miners on the chain employing a PoW consensus algorithm. The information is offloaded to a BC-based cloud for access across multiple domains and reduces the blocks' burden. The cross-domain operations are allowed after the cloud manager verifies it and sends it to the SAM. In the case of frequent accesses, the information is stored in the BC with the same deployment domain. The target difficulty in the model is 17 bits for a SAM device, and the average time consumption decreases with transaction collection time (Tc) with the assumption that there are enough power resources to carry out the verifications. The performance evaluation of the model for cross-domain operations shows that the time consumption in carrying them out is the same during each ½ Tc period. The architecture provides fine-grained auditing, but its performance evaluation runs on various assumptions, such as that all the management domains have the same number of user equipment. The mining is done after the propagation procedure ends, and the SAMs have the same transmissibility to propagate transactions and mining time.

In [139], the authors propose a theoretical architecture for BC-based AC mechanisms with enhanced trust mechanisms and increased portability. The architecture consists of 3 prime layers- Resource layer (RL), BC layer (BL), and Application layer (AL). The model aims to formulate an AC mechanism for defending against attacks in an untrusted environment. The model adopts the PBFT algorithm for consensus, an endorser makes endorsements for the transaction, and a transaction handler executes the chain codes. Users communicate with ALs through a client application for registration and requesting AC. BL is at the core and is deployed on every component in the private network. It consists of 3 components – web controller, transaction handler, and ledger. All the actions such as identity creation, executing access protocol creation, and resource creation happen in the BC. All the requests are saved in the BC in an immutable and non-resistant manner. The model's security analysis shows resistance to AC message tampering until at least 1/3 nodes of the network is not compromised. The model is suitable only for the low-scale implementation and is compromised if the network complexity increases, creating latency and storage problems.

In [140], the authors propose a BC-based AC mechanism for verifying IoT end-points and providing access tokens for querying resources. The architecture is gateway-based, where IoT devices communicate with the gateway instead of the internet, and conversely, any communication to IoT devices goes via gateways. The gateway serves four purposes- protocol bridge, AC, secure communication, and proxy BC. Internet Service Providers (ISPs) act as the gateway approver, vendor device authentication is done by the vendors, and the gateway acts as an authorization server. The AC state is distributed across all nodes and stored on the SCs. A trusted administrator does the SC deployment, and signing of ISPs and vendors. The AC is carried out in a few stages- gateway authentication done by an ISP, vendor authentication of devices by the owner under each domain, and the gateway handles outside requests by verifying and granting access requests. The outside requestors need to build secure channels with gateways before communicating to IoT for access. The ISPs are discredited in case of untrusted behavior, and the domain owner has complete control over the requests coming through the gateway. The model is evaluated over trust, security, and performance. The security analysis shows that the attacks can happen if the attacker leverages massive computational resources, which are costly or compromise the approvers, mitigated by using a certification authority for vendors. The architecture is centralized and needs a trusted intermediary. The authors argue that IoT systems cannot be entirely decentralized and employ trusted approvers for authenticating end-points. The architecture relies on ISPs to route traffic carrying security verifications, while BC provides validation.

In [141], the authors propose an SC-based data sharing and AC mechanism for end-point communication in IoT devices to resolve trust issues. The proposed system consists of SCs for DM in an untrusted environment. Three SCs are used – Access control contract (ACC), Register Contract (RC), and Judge Contract (JC). ACC maintains the AC for any requester and oversees the overall communication AC and data sharing between IoT devices. RC is responsible for the authentication of requests and registers them. The behavioral analysis is done by JC, which checks the node for misconduct and generates alert messages. An ACC is invoked when an AC request is sent, and the request is forwarded based on the access permission level. After objects accomplish the request, the corresponding transaction is stored on the chain. The security analysis shows that the proposed system is open access and secure, and the trustworthiness is maintained throughout using SCs. The model is evaluated against cost and shows that ACC consumes more execution and transaction energy than other SCs.

In [142], the authors propose a BC-based AC mechanism with secure delegation services, an integrated BCT network for eliminating a central delegation service, and

TABLE IV. IoT Security Tasks - Existing centralized and BCT Solutions.

IoT Security tasks	Aim	Existing solutions/Cloud-based solutions.	Existing BIIT solution architectures.
Key Management and Access Control.	Provision of fine-grained AC mechanisms in untrustworthy environments. Applying KM strategies. Trust and authentication	Centralized KM services. Public key Infrastructures. Pre-shared key mechanisms. Key pool frameworks.	BDKMA [138]. Bloccess [139] BorderChain [140] SC-based AC mechanism [141] BACI [142] BPRPDS [143]
Node Authentication	Prevention from false data. Secure device-device communication. Prevention from DoS, Impersonation	RFID- unique fingerprints. Third-party authentication centers. Authentication protocols. Digital signatures. Identity-based cryptography (IBC) Two-factor authentication.	BASA [144] Out of Band Authentication scheme [145] P2P IoT node authentication. [146] Decentralized authentication scheme. [147] BC-based Node Authentication [148]
Data sharing and, Routing security.	Secure exchange of data Prevention of data tampering during an exchange over the network.	Intrusion Detection and prevention methods SDN controllers Cryptographic algorithms for symmetric encryption Hashed-based Security. Network routing protocols. Authorization protocols.	BC based user Authentication [149] MicrothingsChain [150] BC-based security-driven Routing framework [151] Shared memory, BC-based secure and efficient RP [152] LW- BC assisted secure routing of UAS [153]
Prevention of software failures.	Protection from Malware, Spywares, and Adware. Protection from Ransomware. Protection from malicious scripts.	Service contract management Static software-centric approaches for Malware detection. Signature-based detection Anomaly-based detection	IoTMalware [154] B2MDF [155] BC-based distributed anti-malware system [156]
Data storage and management.	Offering reliable data storage. Trust management. Data Loss resilience and Data recovery.	Supervision, Enhance management Platform monitoring Database backup management, Service support platforms. Disaster control and recovery management.	Pdash [157] BC-based Secure storage [158] Design principles for DM [159] BlockTDM [160] BC and DRL based DM [161]

event and query-based services. The device is assigned to a private group, and subsequent permissions are given through a delegation mechanism performed by a BC. The architecture consists of low-powered IoT devices, powered user devices with computation and storage capacity, an application manager for user interface and registration, an IoT manager for data filtering and query management, a BC Manager (BCM) for SCs and AC management. The BCM registers the IoT devices and deploys an SC for each device. BCM allows delegates to activate or deny the permission stored in the SC. The SC stores devices' platform hashes and delegation policies. The BC miners verify before any permission activation. The proposed model is for private networks for increased throughput and reduced latency, but the model cannot be replicated on large-scale IoT systems without affecting the network performance.

In [143], the authors propose a BC-based privacy-preserving and rewarding private data sharing scheme, a BC-based incentive mechanism for private data exchange.The data owner publishes private data and receives a payment anonymously in the BC, while data consumers obtain licenses anonymously through SCs, where licensing technology ensures access control for multi-sharing. The authors leverage Monero technology to ensure the untraceability and unlinkability of DUs while getting private data, ensuring that no one can develop a dat user behavior profile database. The authors incorporate the non-frameability characteristic into the anonymous incentive data sharing scheme. Honest data consumers can refute the frame up using a deniable ring signature without revealing their genuine identity. The authors present the security model, provide the formal security proof using the random oracle model, and demonstrate the model's feasibility in real-time IoT architectures. The authors have proved the effectiveness of their technique and compared it to various undeniable ring signature schemes. The results reveal that the computational cost increases linearly as the number of ring members increases.

In [144], the authors propose an efficient BC-assisted secure cross-domain device authentication mechanism, inducing inter-domain trust and privacy in IIoT applications. Identity-based signatures induce authentication in this mechanism, and privacy is induced by designing the identity management mechanism. The cross-domain authentication privacy perseverance also introduces a key negotiation mechanism to prevent eavesdropping on the insecure channel by negotiating session keys. The architecture consists of four layers.- Entity layer(EL), Agent layer(AL), BC Layer (BCL), and Storage Layer(SL). EL consists of a key generation center (KGC) and IIoT devices. KGC is responsible for the generation of private keys for IIoT devices. AL consists of the BC Agent Server (BAS)and Authentication Agent Server(AAS). The model employs three types of authentication- Unilateral authentication, where users authenticate a device, Mutual authentication, where two devices authenticate each other; and cross-domain authentication, carried by KGC, BAS, and AAS. The domain-specific information is encapsulated into the consortium BC node in transactions and is acquired by other domains for authentication. The authentication agent server executes signature generation and verification operations on behalf of requesting devices. With an increase in the number of endorsing and validating nodes, the BC consensus time increases, introducing latency in the system.

In [145], the authors proposed an out-of-band two-factor authentication scheme to prevent impersonation attacks on large-scale IoT devices using "device relationship" and BCT. The out of band performs the secondary authentication to distinguish home IoT devices from the malicious IoT devices. There are four components of the said authentication scheme- Authentication Subject(AS), which is any device that wants access to resources, Related Device(RD) that performs secondary authentication, BC that stores the 'Relationship information' for every authentication subject with the related device and Authentication Executor (AE) which coordinates the two factors out of band authentication. A relationship contract stores the mapping of AS address to 'Relationship data'. When an AS requests access, AE retrieves the corresponding information from the BC, selects the RD in the AS neighborhood, and sends the corresponding action sequence. The corresponding RD invokes SC to send the verification result to BC, and finally, AE checks BC for verification results utilizing SC. The model has not been implemented on commercial IoT devices due to close-sourced hardware and software, and there are considerable CPU and memory overheads in the authentication stage.

In [146], the authors propose a BC-based authentication mechanism for the low-power sensor nodes that are part of p2p networking using the sequence number of sensor nodes. This paper proposes verification through SHA 64-bit hash function to confirm confidentiality and integrity without compromising performance. The sink node(SN) assigns the sequence numbers by a broadcast-response-based mechanism for registering legitimate devices. The SN keeps a record of the other node's identity in the form of the Ids, sequence number, and hash value; therefore, the sink detects a malicious node by verifying the sequence number and the hash value. A mutual level node authentication model is used where a node and its sequence number store all other nodes' sequence numbers. The node identifies the particular node for communication, compares the corresponding sequence number, and verifies the message by comparing the transmitted hash value. Thus neighbors' hash function detects a malicious node and secures the model from impersonation. However, as the network complexity increases, the sink node has to store many sequence numbers. Further, the sink node acts as a point of failure, and a legitimate node can become corrupt and allow other malicious nodes to transmit the messages.

In [147], the authors propose an authorization and authentication mechanism for LW IoT devices that improve the IoT network's performance. The proposed mechanism is based on the public BC mechanism and uses a fog computing network to achieve the desired task. The system architecture is divided into two layers: the device layer and the fog layer. The device layer consists of the many low-powered and low computational devices responsible for generating the data in the network. The IoT devices can be grouped depending upon the customized functionality they perform. The fog nodes in a particular group perform the same functionality. On the other hand, the fog layer is a BC-enabled fog device connected to the internet for working together. The fog nodes perform the CM execution to validate the transactions and create the blocks. The mechanism proposes three phases -The initialization phase consists of registering the system and devices with the closest BC-enabled fog nodes. The device authentication phase involves authenticating the devices with the BC-enabled fog node by mapping the system ID, device ID, and public address. Device-to-device communication involves the secure transmission of the message between the same system's fog nodes or different systems. Before the device-to-device communication, both the devices are authenticated by the BC-enabled fog node. After that, a block is created in the BC, and subsequently, a secure channel is established between the devices. However, this mechanism assumes that fog nodes and admin are trusted and that communication between fog devices and nodes is secure.

In [148], the authors propose a node authentication model for the IoST(Internet of Sensor Things) based on the BC mechanism. The base station validates any node's credentials whenever it performs any action in the network.The authors have employed identity authentication with PoA as the consensus approach to reduce computational costs. The miners are pre-selected, and following the authentication request, the registered nodes are authenticated.The request contains IDNode(Node ID), MACAddrNode(MAC address), and ReputationNode(the reputation value assigned to a certain node based on its previous history in the network), which are already stored on the BC. The authentication is carried out by comparing the credentials of nodes previously stored in the BC. The BC determines whether or not the credentials provided by nodes match the credentials currently stored in the BC. If the credentials match the information provided, the nodes are authenticated and broadcast as legitimate nodes. A SC is deployed on the base stations that track all the network transactions. The system model is predicated on two assumptions: Firstly, base stations are accepted as legitimate and provide secure services to consumers, and secondly, symmetric keys are securely transferred in the network.

In [149], the authors propose a user authentication strategy based on BC-enabled fog nodes that interface with Ethereum SCs to authenticate users to access IoT devices.The major stakeholders include Administrators(responsible for controlling access permissions for IoT devices), End users(interested in requesting an IoT device service), Fog nodes(for localized storage), and cloud servers(storing IoT data), all having direct access to SCs via an Ethereum client in the case of fog and cloud nodes, or via a front-end application/wallet in the case of administrators and end-users. IoT devices have unique Ethereum addresses (with public and private keys), but they lack connectivity and do not interact with SCs. The system interactions are divided into off-chain and on-chain. In the on-chain interactions, the admin constructs the SCs, registers the IoT devices, maps them to a fog node, and may grant end-users access to certain IoT devices. The SCs check the list of authorized users, and the user receives a SC acceptance token which it uses to authenticate itself off-chain. The authors have provided the security analysis of the architecture,but the cost analysis of utilizing Ethereum-based SCs is unaccounted for.

In [150], propose a decentralized BC-based architecture with SCs to allow edge computing nodes to store IoT data and securely interact with one another.The architecture is composed of 4 layers- Information aggregation layer(consisting of IoT-like devices), Edge computing layer(consisting of edge devices with fair computation capabilities), Service supporting layer(responsible for provision of services), and Application layer.The collaboration with other edge computing nodes must first be certified by the edge computing nodes, which will result in the exchange of MicroCoins(introduced cryptocurrency) between members. The model uses a publish-subscribe mode, allowing users to access data across domains. The users or application developers first subscribe to the data publisher from the edge computing node pool for data exchange. The data publisher then supplies the subscription data and submits a transaction to the BC-enabled SC to manage the pre-set business model while providing the required data. The authors introduce a new CM called Proof-of-Edge computing to reach consensus among all edge computing nodes and avoid centralization. All corresponding operations must be documented in BC to obtain self and other domain audits.

In [151], the authors propose integrating Network Function Virtualization(NFV), software-defined network(SDN), and BC to create a flexible and reliable routing architecture for IIoT. SDN and NFV are responsible for creating programmable forwarding devices that create the network's optimal routing policies. The controllers are secured using BCT and take decisions and collect the data from the nodes to detect mistrust. A secure path is acquired by adequately removing the malicious node from the IIoT network by periodic monitoring and collecting network data. Each controller has a distributed ledger, and malicious nodes are identified by calculating the network's trust value during behavior authentication stored in the BCs. The synchronization reaches a consensus among various ledgers transmitted through a control channel. Different controllers handle routing requests through an access point. The experimental evaluation shows that the model outperforms the state-of-the-art systems in average delay over attacks and packet loss rate. However, the frequent calculations of trust values lead to substantial computational power, bringing overheads in the system, which must be addressed without compromising the model's security.

In [152], the authors propose a routing protocol for the wireless sensor network that uses BCT to make routing more efficient and secure. The nodes present in the network are treated as the coins, and the routing path for the message is treated as the transaction, which is subsequently added to the BC. Initially, all the nodes are owned by the sink and considered inactive, and the rest are active. When an event occurs, the nodes access the BC to find the optimal path to the sink. Dijkstra's algorithm obtains the message's optimal path by a cost function determined by signal and interference. This optimal path is the transaction to be added to the BC and transmit the message after eliminating malicious nodes detected by the BC security mechanism. The routing process is made secure by trusted cryptographic algorithms such as ECDSA224 and SHA512. While transmitting the message to the sink, the node seeks the 'ownership' of the path's nodes transferred back after successfully sending the message. However, the model assumes that all nodes are homogenous and that the sink has enough resources to handle the messages. Complex calculations are involved in finding routes that increase the computational overhead and network cost.

In [153], the authors propose a BC-assisted secure routing algorithm for a network based on 5G new radio for the swarm Unmanned Aircraft System(UAS) to prevent the disruptive attacks committed on UAS networking. The BC performs two main functions -Selecting the secure next hop for transmission of a packet from one to another and the authentication and verification of UASs. The BC distributed updated block digests to the whole swarm after a UAS is authenticated. The BC used is LW, which is different from the conventional BC distribution. Instead of using conventional mechanisms, the traffic status of UASs is leveraged to achieve a consensus known as Proof of Traffic(PoT). The neighborhood of UAS is decided based on the destination and record of the digest in BC, and each UAS in the swarm delivers packets to its neighbors with beamforming. The block digest records are checked so that the unauthenticated UAS are not chosen as hops. The attackers need the specific BC digest to launch an attack, which is computationally very expensive. PoT employs the passive broadcast for block synchronization, unlike conventional algorithms, which reduces the system's overheads suitable for LW environments. However, the model assumes that the hackers cannot compromise a UAS in joining the swarm UAS networking. The untrusted UAS cannot recuperate the signal with side lopes leakage of beamforming without directional transmission.

In [154], the authors propose a malware detection technique in IoT devices using Deep Learning (DL)and BCT, where SCs detect malicious applications. SC guides users' and end-developers' interactions, stores information about new apks, and enables tracking of malicious apps on the network. The malware features are shared and trained on DL models in android IoT devices. After the user uploads an app to the network, it is stored in an IPFS where the DL models extract features. The hash values obtained from the training models are stored in an immutable fashion on a BC network to prevent decompilation and repacking attacks by reverse engineering methods. When a user downloads a new app, the user sends the hash to the network for verification, where an SC decides whether the app is malicious or not. The model has been evaluated on 18,850 android applications and 10,000 malware android packages and shows considerable efficiency. However, the analysis of bandwidth consumption by the IPFS based storage is not given, which is important, especially in the case of metered connections In [155], the authors propose a BC-based framework for detecting malware in mobile applications before downloading. The model relies on dynamic and static analysis for detecting malware. The model uses two external and internal BCs. The internal private BC(IPB) contains feature extractors(FEs) to extend the dedicated internal private BC(DIPB). FE extracts information during the lifetime of an app. These features can be static, extracted from the file, or dynamic and extracted by monitoring the run time behavior. Each FE component is connected to a DIBP that tracks each app using the behavioral information. A dedicated external private BC(DECB) for each application contains scanning information of application versions. A determinant agent(DE) is part of the BC and based on the data in the BC, it classifies the app as malicious or not. DEs attach their decisions to DEPBs with relevant information. Although the dedicated BC for each app reduces the computational burden of one BC, it also increases the system's overall complexity.

In [156], the authors propose a distributed anti-malware protection mechanism to support a hybrid signature and anomaly-based detection model. When a new file is added, the users make a signed hash of the file corresponding hash is sent to the BC ledger. The verification is done on signature-based detection, and the system process and ports are checked for malicious activity. However, the signature-based verification suffers from detection evasion if the hash of the malicious file is changed. To avoid this, if the hash comparison does not match, a notification is sent to the users, and the system process and network ports are continued to be examined. If any suspicious activity is found, the file is blocked from self-executing. The BC is updated with the hash of the malware file detected. This can prevent DDoS attacks where the malicious app may attempt to gain access to IoT devices. However, the proposed mechanism is suited for servers at the application layer for personal computers and servers but not for resource-constrained IoT devices.

In [157], the authors propose a three layer parallel distributed architecture for storing and sharing IoT data-BC layer, Node layer, Distributed storage layer aimed to improve the scalabilty of BC-based systems. The data generated by IoT devices is encrypted, and the hash value of the data is generated and stored in the BC as its unique identity. BC is the system's control layer and is responsible for validating transactionsand data access control and also provides a platform for SCs to support various applications. The raw data is encrypted locally and stored in multiple storage nodes across the distributed network using the Kademlia method so that the data host has no access to the original data. The encryption technique used is AES (Advanced encryption standard). The data owner adds a digital signature to the data block's digest, allowing the data's ownership to be authenticated. The efficiency analysis reveals that in a network of 2n nodes, retrieving any data requires a maximum of n steps.

In [158], the authors propose a BC-based solution for the decentralized storage mechanism and secure data transmission, in this case, a sensing image, in IoT networks. This paper proposes using an encryption algorithm for secure data transfer and an intelligent verification algorithm for data storage and signature verification. A blocking algorithm is employed for sensing an image, and an intelligent sensor divides the image using image sensing and block data partitioning. A public key generation algorithm is leveraged, and the smart image sensor securely transmits the key information to BC. The sensor signs the data blocks with different keys at different intervals and transmits the message to the server, where a signature verification algorithm is employed. If the signature is verified, the data block is stored. The theoretical analysis shows that the model is resistant to counterfeit, theft, replay, and DoS attacks. The BC uses only one public key to authenticate different blocks, reducing the cost, but the intelligent sensor calculates n+1 keys for n blocks and stores n keys.

In [159], the authors propose a theoretical prototype of BC-based IoT architecture using a design science research approach. The approach aims to design a prototype for data center decision-making, simplicity, complete digitization, tamper resistance, heterogeneity, and authentication of BC data. The Raspberry Pi is configured as a client node for the Ethereum BC, containing the storage and computational configuration layer. The model has three prime components- IoT data logger(senses the data), SCs (stores data, chain address of the devices, and records events), and the monitoring dashboard component(displays data to end-users, communicates with the SCs, and behaves as a mining node). The system considers Ethereum BC, where SCs are executed on a virtual machine to reduce costs. The accounts on Ethereum are classified as contract (contain balance and contract storage executed via a transaction sent to its unique address)and externally owned(refer to external agents and contain only balance). The prototype is designed for high data availability, parsimony, and modularity in IoT ecosystems essential for efficient DM, but the design encounters high operational costs and scalability issues.

In [160], the authors propose a trusted DM scheme for sensitive data distribution and storage in EC. The architecture is divided into three layers- Edge device(Fog nodes), BC Network(to which data is committed), Edge nodes(provides services), and Cloud center layer(complex problem solving). BlockTDM is reliant on a multi-step mutual authentication scheme based on certificates. A modified PBFT - broadcast multi-signature-based CM is employed where a client commits the message to the endorsing pairs (EPs) and the management pair(PM). PM verifies the signature, the endorsing pairs simulate, and the result is broadcasted to an ordering service peer and delivered to the bookkeeper. A multichannel matrix-based architecture is considered for data protection for blocks on different channels and user-defined data encryption for interchannel security. The scheme employs Hyperledger Chaincode as an SC connected to the EPs and is invoked to process transactions and query over the protected BC data. SCs are designed for data of various kinds, such as multimedia and documents, to support specific block DM. The model is highly secure but has O(n^2) communication complexity.

In [161], the authors propose a BC and Deep reinforcement learning(DRL) based scheme for efficient DM to achieve high-quality data collection with limited mobile terminal (MT) energy resources and sensing range and secure data sharing in Industrial IoT. The model proposes collecting the data through a DRL approach fed to the BC network. The connection of each MT is validated, and data is encrypted using keys and digital signatures. BC integration ensures data security and reliability when MTs share data and prevents the systems from attacks. Multiple Ethereum nodes are distributed across a private chain that interacts with the SC deployed on the chain. A certification authority is set up to maintain the data's reliability and authenticity to avoid fraudulent transactions by MTs. The model is tested on the severity of DoS and DDoS attacks, and it is that DDoS attacks have a 0.1 % worse impact than DoS attacks. The increase in MTs does not impact the network, but both the attacks affect the database as the transaction frequency increases affecting the data storage.

1) *Critical Analysis of the proposed architectures:*

The evaluation of these studied techniques reveals that a tradeoff exists between IoT security and other performance criteria. Most of the proposed frameworks have been carefully verified against several security metrics, but the cost issues for customers or businesses are not addressed. The model in [145] cannot be implemented on commercial IoT devices due to close-sourced hardware and software, and there are considerable CPU and memory overheads in the authentication stage. In the architecture presented in [146], the sink node has to store many sequence numbers as the network complexity increases. In [151], the frequent calculations of trust values lead to substantial computational power, bringing overheads to the system. In [152], complex calculations are involved in finding routes that increase the computational overhead and network cost. In [154], the analysis of bandwidth consumption by the IPFS-based storage is not given, which is important, especially in the case of metered connections. In [155], the dedicated BC for each app increases the system's overall complexity. In [160], the model has a communication complexity of O(n^2). Many architectures have ignored or not completely addressed the issues of latency, scalability, energy consumption, computational power, or the security aspect of privacy leakage. Most methods restrict to a certain aspect of IoT security while ignoring the computational overheads of implementation on a large scale. The architecture of [139] is suitable for the low-scale implementation, but the network performance is compromised if the network complexity increases, creating latency and storage problems. The model is resistant to AC message tampering until one-third of the network is not compromised. The proposed model in [142] is for private networks and cannot be replicated on large-scale IoT systems without affecting the network performance. The architecture proposed in [144] suffers from latency issues when the number of endorsing and validating nodes increases. The design in [159] encounters high operational costs and scalability issues.

The authentication, trustworthiness, and authorization in many BC-based architectures are achieved through SCs, introducing transactional costs. In [141], ACC consumes high execution and transaction energy. In [149], the security analysis is provided in-depth, but the cost analysis of utilizing Ethereum-based SCs is unaccounted for. Many architectures provide security but are not suitable in constrained environments. In [156], the proposed mechanism is suited for servers at the application layer for personal computers and servers but cannot be replicated for IoT devices.The architectures are not truly decentralized and run on some form of central scheme and are prone to security issues. In [146], the sink node acts as a point of failure, and a legitimate node can become corrupt and allow other malicious nodes to transmit the messages. BC-based systems incur high storage costs too. In [161], the increase in MTs does not impact the network, but both the attacks affect the database as the transaction frequency increases affecting the data storage.

Many architectures rely on assumptions that may not be practically true. The architecture presented in [138] runs on various assumptions, such as that all the management domains have the same number of user equipment, the mining is done after the propagation procedure ends, the SAMs have the same transmissibility to propagate transactions and mining time and that there are enough power resources to carry out the verifications. The architecture of [148] runs on the assumption that base stations are always legitimate and that symmetric keys are securely transmitted in the network. In [147], the mechanism assumes that fog nodes and admin are trusted and that communication between fog devices and nodes is secure. In [152], the model assumes that all nodes are homogenous and that the sink has enough resources to handle the messages.

B. Security benefits of BIIT systems :

Despite the limitations, there are significant benefits of BIIT systems. The information created by IoT frameworks is broadly significant and confidential, and BCT substantially increases the security in distributed networks. BIIT systems offer the following security merits:

1) Data integrity and confidentiality: The transactions in BIIT systems are verified through a CM, and all the nodes have an identical copy of the ledger. The data and transactions are highly encrypted by leveraging cryptographic mechanisms intrinsic to the BC.
2) Data provenance: BIIT systems offer traceability by keeping a historical record of the timestamp in the BC.
3) Fault tolerance: In BIIT systems, the data is distributed across multiple devices, and a single node failure does not disrupt the system's functionality. This eliminates a single point of failure and makes the BIIT systems more robust than centralized IoT systems.
4) Secure communication and resistance to attacks: CM prevents the malicious nodes from corrupting the system. Launching an attack requires leveraging high computational resources.
5) Trust management: BCs bring trust in the communicating nodes and, through SCs, provide rules that guide a user's authorization. SCs invoke clauses in the event of mistrust and penalizes the user for the breach.
6) Access control: BIIT systems provide uniform access across multiple IoT systems. In BIIT systems, the IoT device is coupled with a unique identifier, and efficient KM and AC mechanisms for interoperability are available.
7) Removing third-party risks: BCs decentralize the structure authority and provide secure DM with a decentralized architecture. Thus, the data is not under the control of a private organization but distributed across a plurality of nodes.

BIIT systems offer higher security than centralized IoT architectures. A comparison is given in Table V.

9. Challenges, Open Issues, and Research Directions:

BCT is emerging as a key paradigm for establishing trust, imparting security, auditing capability, and verifiability in systems. BIIT systems are secure but require a scalable architecture with sufficient throughput and low latency. IoT systems are constrained, and designing less intensive security measures for low-powered devices with low storage, computational, and network overheads are in progress. The constrained nature of IoT and other factors hinders the deployment of BIIT systems, briefly discussed below:

1) Cost of IoT storage through SCs: In Ethereum SCs, the amount of computational work required to complete an operation in a transaction is measured in Gas units. The currency to pay for Gas units is Ether/ gwei (1 gwei= 10-9 ethers). There is no fixed price set for the gas, and the sender enforces a gas limit in the transaction and specifies the gas cost. Miners mine the blocks which specify high gas prices. The price of Ethereum has risen from a single-digit USD value in 2015 to touching 2500 USD in 2021 [162]. Suppose a transaction requires 100 million gas units with 1 gas unit set at 25 gwei; the corresponding price in dollars to complete the transaction would be 108x25x 10-9x2500=6250 USD. With more devices in the network, data storage complexity also increases. BCs store an immutable, permanent record of data, and with the increase in the nodes, the size of the chain also increases, which causes storage/memory concerns. Although BC eliminates the management costs in a system, it is considerably expensive to store data in a BC. Ethereum costs 76000 USD per GB, which is very expensive for

TABLE V. Evaluation of network security - Existing centralized architectures Vs. BIIT architecture

IoT Network level	Security issues	Evaluation of IoT Network Security	
		Existing network/ Cloud architecture of IoT	BIIT architecture
Application Layer .	Software failures	Weak operating systems and Vulnerable application software.	StrongOperating systems Tested applications
	Malware attacks	Evasion of anti-malware schemes. Late/ False detection.	Secure storage of Malware information.
	AC and Identity Authentication.	Weak AC mechanisms.	Fine-grained hierarchical AC mechanisms.
	Data protection	No encryption for data at rest.	Strong encryption for Data at Rest and data communication.
	Data Loss	Vulnerable third-party software modules. Hackable centralized servers. Susceptible to data leakage.	Decentralized and distributed modules. Robust architecture.
Network Layer	Phishing	Vulnerable to Centralized attacks.	Secure exchange of data between platforms.
	Interoperability	Not suitable for cross-domain authentication.	Inter-domain authentication. Multiple domain access. Cross-domain operations
	Confidentiality	Unauthorized access.	Data confidentiality is maintained.
	Routing security	Non –Robust routing information.	Traceable and tamper-proof routing information
	Data security	Susceptible to Channel attacks such as Replay attacks, Man in the middle attack, Impersonation, Ephemeral secret leakage.	Secure exchange of data between platforms. Trusted routing environment.
Perception Layer	Key Management	Strong dependence on the third party for KM. Vulnerable to Privacy breaches.	Secure distribution of keys Privacy preservation.
	Data protection	Susceptible to security attacks. Data repudiation. DoS.	High Data Security.
	Mass node authentication	Reliance on third-party authentication centers.	Distributed and decentralized authentication mechanisms. Consensus-based Authentication.
	Dynamic nature of IoT topology	Heterogeneity hinders Security.	Transformation of heterogeneous data into a uniform format.
	Protection from false data	Susceptible to data tampering and leakage.	Traceable data. Data tampering is costly. Auditability.
	Encryption	Scalability issues while employing digital signatures.	Highly encrypted data.

IoT applications. The research is moving towards cost analysis and solutions for IoT storage through BC SCs. In [163], the authors investigate the storage costs of numeric data on BC through SCs. The data storage is conducted using two strategies. In scenario 1, the data is stored in an array, and in Scenario 2, the data is encoded into one variable using two methods- Encoding within SC and encoding outside SC. The experimental results show that encoding the data outside SC into one variable is cost-efficient compared to storing data in an array or encoding it into a variable within SC.

2) Power consumption: IoT devices applyenergy-saving strategies such as “Sleep and Wake up” scheduling to increase the network lifetime. However, due to BC’s unique way of storing and continuous data processing, the energy consumed by such a system is considerably higher than conventional systems. The authors in [164] estimate the energy consumption of various cryptocurrencies. The processing power is measured in hash rates. Bitcoin uses SHA-256 and has a rated power network of 4291,366 KWwhich an IoT node cannot support. Mining is computationally expensive, which necessitates specialized machinery and massive quantities of electricity.It is challenging to run BC as a full node on IoT devices. Recent solutions suggest using edge computing to enable mobile devices to offload the mining work to the cloud. Edge computing can be incorporated to help mobile devices offload mining work to cloud resources. The authors in [165] propose a 4-layer BC-based framework for IoT where the devices and servers participate in BC via p2p communication. The end devices handle simple operations while more powerful servers support the complex operations in the top tiers at the edge/cloud.

3) Network model in BC systems: The expansion of the BIIT system creates new requesting blocks. The requesting block and the state data must lead to a consistent system state, and the newer clients synchronize with the existing state. The majority of the BC-based traffic models are p2p. The authors of [55] categorize it into three types- Gossip Protocol, Kademlia Algorithm, and DAG. The gossip-based BCs offer relatively less latency and energy consumption but achieve data integrity at the cost of large message overheads [166]. The Kademlia algorithm works with lesser communication overhead, and the resource location in DAG is guaranteed. Ethereum also employs p2p networking with no trusted intermediary. The nodes themselves act as the service and the service providers to ensure data synchronization [167]. Ethereum follows a discovery protocol that allows the nodes to find each other. BlIT systems must satisfy consistency in an asynchronous network with reduced latency and increased security. The security of consensus depends on the underlying network. Studying the network extensively to determine what affects the performance of a p2p network is an important issue. In [168], the authors study the network structure of Ethereum by running a customized version of Ethereum’s Go client, GETH, for seven months.

4) BC Security and Privacy vulnerabilities: BC-based systems provide high security to systems by making data tamper-proof. However, BC itself exhibits security vulnerabilities. The adversity tolerance is further reduced with modifications in CMs for LW environments. Common security threats to BC include Protocol attacks, Ellipse attacks, the chance of double-spending, Consensus protocol attacks, SC Vulnerabilities, Programming frauds, Private Key Leakage, DDoS attacks, and other security issues[169], [170]. Employment of communication security protocols such as Datagram transport layer security is resource-intensive and not suitable. Further, all transactions in the BC are transparent. By analyzing the patterns of transactions from a user, the anonymity of a user can be compromised and lead to potential front-running. For private communications, protocols such as Telehash or Whisper can be integrated. Privacy leakage can be countered through privacy protection mechanisms such as Zero-knowledge proof, Attribute-based Encryption [171]. However, these cryptographic algorithms are highly resource-intensive and unaffordable in LW environments.

5) SC Vulnerabilities: A fault in the SC could be caused by a simple typing error, a misinterpretation of the specification, or a more severe programming error. BC is irreversible, and a minor glitch has many ramifications for SC security and functionality. For example, the quantity of gas that the transactions contained in the block can utilize is limited to prevent the chains from growing beyond a point. If data is stored in variable-sized arrays and accessed through loops, the gas can get exhausted before committing a transaction. Miners are compensated, but the transaction is reversed. As a result, testing mechanisms for SCs is a critical problem. The test mechanism must inspect the SC on enough data for all malicious and non-malicious inputs before deployment to detect anomalies. Furthermore, because IoT systems are distributed across multiple locations, retrieving data from various sources can cause the SCs to become overburdened. It’s difficult to fine-tune SCs for IoT LW applications. SCs are associated with a variety of other challenges. The legal enforcement of SCs, for example, is currently restricted. Dual integration of SCs with real-world legal contracts is one solution that has been proposed.

6) IoT specific Consensus: The abilities of the existing CMs are limited when applied to IoT and have not been tested thoroughly. Conventional CMs, such as PoW, is resource-intensive and cannot run on IoT devices. Even a powerful IoT node such as Raspberry pi3 can only achieve 104 hashes per second,

while a Bitcoin network can conduct around 1019 hashes per second. Integration of full BC nodes in IoT is in the nascent stage. Malicious attacks on lightweight CMs with low adversity tolerance can prevent valid transactions. A potential solution is to limit the consensus to the edge / decentralized cloud, while IoT nodes save only the hash values, but this increases the storage overheads on the edge. Furthermore, the interoperability and authentication standards for edge devices are limited.

7) Throughput, Latency, Scalability, and Network complexity:BC systems do not scale well if the network size increases massively. The network efficiency reduces as the network scales up and more authentication requests are handled, leading to network congestion. The growth of the chain further leads to bandwidth problems. The mobility of IoT devices also affects BC performance. BCs are inherently latency tolerant, and the mining time is induced to secure the networks further, which is unacceptable in real-time IoT systems such as IoV. A potential solution is to integrate IPFS, AI, and ML to complement the BC. Off-Chain solutions can be integrated to increase the transaction throughput. IoT big data is posing challenges in real-time data delivery. Integration of ML in BIIT systems for IoT Big data analytics is hindered by storage, latency, scalability, and other challenges. Further investigation is required to analyze the overheads introduced in BC-IPFS integration. Normalization and compression techniques explicitly designed for BIIT systems where BC power is leveraged are required.

8) Compatibility and Adoption: BC is an emerging technology and lacks standardization laws. Access control legislation is an issue in public BCs. IoT data is heterogeneous, and the diversity of IoT devices implies the need for different network protocols. Protocol conversions to enable smooth communication are especially costly in BIIT systems. The large-scale adoption of BIIT applications needs significant infrastructural changes. A generic BC-IoT architecture is needed to bridge the gap between IoT service providers and BC. IoT service providers must modify the underlying naming and discovery schemes to comply with the BC mechanism. Laws and regulations concerning information security govern the IoT domain, and many countries have strict legislative rules regarding cryptocurrencies.

A. Research Directions

We present the following research directions based on our thorough study of the domain.

1) 1. Cost reduction strategies: The rising cost of Ethereum is impeding the use of BC in IoT. More research into strategies to lower the cost of BC adoption in IoT is needed. Given IoT Big data's concerns, more efficient data representations that allow low-cost SC operations require further investigation to make large-scale IoT-BC systems commercially viable.

2) IoT-BC Traffic Models: Performing large-scale data collection and traffic analysis of growing-BC chains is an understudied topic due to large-scale simulation and time requirements. The security of the consensus protocols is based on the assumption of efficient p2p overlay network operations. More research is needed to understand the parameters that influence the properties of p2p networks.

3) Testing Mechanisms for SCs: The voids in the SCs can expose BC security. SCs are vulnerable to mining pool attacks because they are open source to all parties involved. Once deployed, the SC is irreversible and cannot be repaired in the event of a virus or a hacking attack. Thus, validating and devising unerring testing mechanisms for SCs and running them on sufficient data is an important research direction.

4) At the Edge Consensus: IoT devices have limited computational and networking capabilities; thus, running BC as a full node is difficult. It is critical to protect IoT suitable CMs from attackers from gaining control of the majority of hash power. Designing IoT suitable mechanisms with good adversity tolerance and low latency is an open issue and a strong research direction.

5) Integration with computing platforms:Due to the constrained nature of IoT devices, Fog /Cloud servers are added at top tiers, storing the entire BC information for transaction validation. It is necessary to enable IoT devices to push transactions to the BC without centralized block endorsement groups. Designing architectures for such integration without compromising the security and privacy concerns is a strong research direction.

6) Network Configuration: There is no standard architecture for BIIT systems. Integration of the cloud and the edge at a higher level is critical. Configuring BCs at the node, edge, and cloud levels and load balancing and network congestion control for addressing increased validation requests are open research issues.

7) Convergence of BC and ML: BC-based systems can benefit from the addition of MLalgorithms. SCs can be used to create a reward-based mechanism for training ML models. The potential of ML-BC integration has yet to be fully realized, but it is a promising future direction.

8) Convergence of BC and IPFS: With IPFS, BC only saves the cryptographic hashes slowing down the chain development drastically. Through SCs, BC can allow access-controlled file sharing and secure storage of cryptographic hashes of IPFS. It is crucial to analyze the latency introduced in the IPFS primarily due to the contact with BC and the consequences on LW operations.

9) Securing BC and Transactional privacy: Pattern analysis of transparent transactions exposes users' privacy. More research is needed to protect BC-based AC systems from security threats. Thus, a potential research direction is developing LW cryptographic algorithms for BCs to protect transactional and user privacy in BC-based IoT systems.

10. Conclusion

The disruptive attacks on IoT networks are predicted to be more severe in the future due to the advanced capability of B5G and 6G networks. The unique properties of BCT for enabling a p2p network with no centralized stakeholder controlling the system enable it to be a perfect security solution. BCs, through SCs, provide fine-grained AC by providing global functions of authentication, authorization, and KM, besides providing a distributed architecture for secure storage of hashes, verification rules, sensor data, and other information. However, IoT devices are constrained and require an LW implementation of CMs to bear the computational, storage, power, and network overheads. This paper presents a comprehensive comparison of BC solutions for IoT systems and concludes that BC can provide efficient KM and AC, node authentication, routing security, and securely store the domain-specific information. A detailed survey of recent research on security enhancement, consensus, applications, integration with ML, and computing platforms is presented. We discuss IPFS, ML, and EC can facilitate BC as a crucial enabling technology for IoT. Through IPFS-enabled BCs, the growth of the chain is restricted by only storing hashes on the BC, and the AC list is maintained by SCs, enforced by the updated IPFS software. MEC is being considered to be a potential approach for achieving consensus for mobile users, facilitating BC applications in future mobile IoT systems.

The convergence of BC and ML for IoT can enable accurate data analytics. 6G systems are expected to create a massive convergence of IoT, AI, EC, Quantum ML, and BCT for fast and secure systems that can support a plethora of devices. IoT systems are rapidly evolving, and as the number of network nodes grows, the tradeoffs between energy consumption, security, latency, throughput, and scalability become more complex. We conclude that BC and IoT technology have evolved separately and for futuristic IoT systems to reach their full potential, extensive research is needed in two domains- a) Blockchain as enabling technology in IoT and b)Enabling technologies for BC-based IoT. Challenges such as the rising cost of Ethereum, power consumption of IoT nodes, SC security, and legislation issues are hindering the large-scale adoption of BC-based IoT. Extensive research is needed on the parameters affecting the network properties, cost reduction strategies, encoding, traffic modeling, off-chain solutions, network configuration, transactional privacy, SC testing, and BC security, especially in LW environments.

References

[1] "The internet of things (iot) technology - ericsson." [Online]. Available: -https://www.ericsson.com/en/internet-of-things

[2] D. S. Linthicum, "Connecting fog and cloud computing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 18–20, March 2017.

[3] S. Showkat and S. Qureshi, "Securing the internet of things using blockchain," in *2020 10th International Conference on Cloud Computing*, D. S. E. (Confluence), Ed., January 2020, pp. 540–545.

[4] F. Gao, D.-L. Chen, M.-H. Weng, and R.-Y. Yang, "Revealing development trends in blockchain-based 5g network technologies through patent analysis," *Sustainability*, vol. 13, p. 5, January 2021.

[5] P. K. Sharma, M. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[6] B. C. al., "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, November 2019.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[8] T. A. Butt and M. Afzaal, "Security and privacy in smart cities: Issues and current solutions," *in Smart Technologies and Innovation for a Sustainable Future, Cham pp*, pp. 317–323, 2019.

[9] A. Verma, A. Khanna, A. Agrawal, A. Darwish, and A. E. Hassanien, "Security and privacy in smart city applications and services: Opportunities and challenges," in *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*, A. E. Hassanien and M. Elhoseny, Eds. Cham: Springer International Publishing, 2019, pp. 1–15.

[10] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' iot communications," *Transactions on Emerging Telecommunications Technologies*.

[11] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and smart healthcare security: A survey," *Procedia Computer Science*, vol. 175, pp. 615–620, January 2020.

[12] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," *Global Health Journal*, vol. 3, no. 3, pp. 62–65, September 2019.

[13] S. Zeadally, F. Siddiqui, Z. Baig, and A. Ibrahim, "Smart healthcare: Challenges and potential solutions using internet of things (iot) and big data analytics," *PSU Research Review*, vol. 4, no. 2, pp. 149–168, January 2019.

[14] C. Bekara, "Security issues and challenges for the iot-based smart grid," *Procedia Computer Science*, vol. 34, pp. 532–537, January 2014.

[15] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, June 2019.

[16] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, p. 1, March 2019.

[17] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "Iot based smart home: Security challenges, security requirements and solutions," in

2017 23rd International Conference on Automation and Computing (ICAC, September 2017, pp. 1–6.

[18] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an iot based smart home," *in*, vol. 2017, no. 40, pp. 1292–1297, May 2017.

[19] Z. Shouran, A. Ashari, and T. Priyambodo, "Internet of things (iot) of smart home: Privacy and security," *International Journal of Computer Applications*, vol. 182, pp. 3–8, February 2019.

[20] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-things (iot)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 29 551–12 958, 2019.

[21] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32 031–32 053, 2020.

[22] X. Y. al., "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, February 2021.

[23] Y. S. al., "Attacks and countermeasures in the internet of vehicles," *Ann. Telecommun.*, vol. 72, no. 5-6, pp. 283–295, June 2017.

[24] H. Xu, J. Lin, and W. Yu, "Smart transportation systems: Architecture, enabling technologies, and open issues," in *Secure and Trustworthy Transportation Cyber-Physical Systems*, Y. Sun and H. Song, Eds. Singapore: Springer, 2017, pp. 23–49.

[25] L. Alouache, N. Nguyen, M. Aliouat, and R. Chelouah, "Survey on iov routing protocols: Security and network architecture," *International Journal of Communication Systems*, vol. 32, p. 2, 2019.

[26] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable iiot critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, February 2021.

[27] M. H. Miraz and M. Ali, *Applications of Blockchain Technology beyond Cryptocurrency*. [cs], 2018.

[28] F. Glaser, "Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis," 2017.

[29] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

[30] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li, and C. Yuan, "A study on the optimization of blockchain hashing algorithm based on prca," *Security and Communication Networks*, vol. 2020, September 2020.

[31] T. M. Fernandez-Caramas and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[32] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, October 2019.

[33] Y. Liu, J. Zhang, and J. Zhan, *Privacy protection for fog computing and the internet of things data based on blockchain*. Cluster Comput.

[34] S. Ferretti and G. D'Angelo, "On the ethereum blockchain structure: A complex networks theory perspective," *Concurrency and Computation: Practice and Experience*, vol. 32, p. 12, 2020.

[35] F. Chen, Z. Xiao, L. Cui, Q. Lin, J. Li, and S. Yu, "Blockchain for internet of things applications: A review and open issues," *Journal of Network and Computer Applications*, vol. 172, December 2020.

[36] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," *[cs], Feb*, vol. 2020, Apr. 2021. [Online]. Available: http://arxiv.org/abs/2001.07091

[37] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *The Review of Financial Studies*, vol. 32, no. 5, pp. 1754–1797, May 2019.

[38] T. H. al., "Transaction-based classification and detection approach for ethereum smart contract," *Information Processing Management*, vol. 58, p. 2, March 2021.

[39] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey," *Sensors*, vol. 22, no. 3, p. 1094, 2022.

[40] ""electronics | free full-text | blockchain for iot applications: Taxonomy, platforms, recent advances, challenges and future research directions."."

[41] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: approaches, opportunities, and future directions," *Future Generation Computer Systems*, 2022.

[42] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure iot: Background, integration trends and a way forward," *J. Netw. Comput. Appl.*, vol. 181, May 2021.

[43] A. K. Paul, X. Qu, and Z. Wen, *Blockchain-a promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues*. Peer Peer Netw. Appl.

[44] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54 478–54 497, 2021.

[45] P. Patil, M. Sangeetha, and V. Bhaskar, "Blockchain for iot access control, security and privacy: A review," *Wirel. Pers. Commun.*, vol. 117, no. 3, pp. 1815–1834, April 2021.

[46] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in internet of things environment," *Comput. Commun.*, vol. 163, pp. 109–133, November 2020.

[47] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Comput. Commun.*, vol. 160, pp. 475–493, July 2020.

[48] J. Sengupta, S. Ruj, and S. D. Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot,” *J. Netw. Comput. Appl.*, vol. 149, January 2020.

[49] B. Alotaibi, “Utilizing blockchain to overcome cyber security concerns in the internet of things: A review,” *IEEE Sens*, vol. 19, no. 23, pp. 10 953–10 971, December 2019.

[50] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, May 2020.

[51] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, “A comprehensive survey of blockchain: From theory to iot applications and beyond,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, October 2019.

[52] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the internet of things: A comprehensive survey,” *IEEE Commun. Surv. Tutor*, vol. 21, no. 2, pp. 1676–1717, 2019.

[53] A. K. Yadav and K. Singh, “Comparative analysis of consensus algorithms of blockchain technology,” *in Ambient Communications and Computer Systems, Singapore pp*, pp. 205–218, 2020.

[54] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, “A survey of blockchain consensus algorithms performance evaluation criteria,” *Expert Syst. Appl.*, vol. 154, September 2020.

[55] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, “A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling,” *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–18, February 2020.

[56] Y. Wen, F. Lu, Y. Liu, P. Cong, and X. Huang, “Blockchain consensus mechanisms and their applications in iot: A literature survey,” *in Algorithms and Architectures for Parallel Processing, Cham pp*, pp. 564–579, 2020.

[57] M. Salimitari, M. Chatterjee, and Y. P. Fallah, “A survey on consensus methods in blockchain for resource-constrained iot networks,” *Internet of Things*, vol. 11, September 2020.

[58] M. Salimitari and M. Chatterjee, “A survey on consensus protocols in blockchain for iot networks,” *[cs], Jun*, vol. 2019, Apr. 2021. [Online]. Available: http://arxiv.org/abs/1809.05613

[59] H. Rathore, A. Mohamed, and M. Guizani, “A survey of blockchain enabled cyber-physical systems,” *Sensors*, vol. 20, p. 1, January 2020.

[60] A. Pieroni, N. Scarpato, and L. Felli, “Blockchain and iot convergence-a systematic survey on technologies, protocols and security,” *Applied Sciences*, vol. 10, p. 19, January 2020.

[61] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, October 2019.

[62] P. Mehta, R. Gupta, and S. Tanwar, “Blockchain envisioned uav networks: Challenges, solutions, and comparisons,” *Comput. Commun.*, vol. 151, pp. 518–538, February 2020.

[63] U. Bodkhe, S. Tanwar, P. Bhattacharya, and N. Kumar, “Blockchain for precision irrigation: Opportunities and challenges,” *Trans. Emerg. Telecommun. Technol., p. e*, vol. 4059.

[64] M. Torky and A. E. Hassanein, “Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges,” *Comput. Electron*, vol. 178, November 2020.

[65] S. E. Chang and Y. Chen, “When blockchain meets supply chain: A systematic literature review on current development and potential applications,” *IEEE Access*, vol. 8, pp. 62 478–62 494, 2020.

[66] P. P. Ray, D. Dash, K. Salah, and N. Kumar, “Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases,” *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, March 2021.

[67] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, “Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges,” *J. Netw. Comput. Appl.*, vol. 181, May 2021.

[68] M. B. M. al., “Blockchain for the internet of vehicles towards intelligent transportation systems: A survey,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, March 2021.

[69] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, “Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges,” *Mechanical Systems and Signal Processing*, vol. 135, January 2020.

[70] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, “Edge intelligence and blockchain empowered 5g beyond for the industrial internet of things,” *IEEE Network*, vol. 33, no. 5, pp. 12–19, September 2019.

[71] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W. Hong, “Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward,” *IEEE Access*, vol. 8, pp. 474–488, 2020.

[72] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, “A survey on boosting iot security and privacy through blockchain exploration, requirements, and open issues,” *Cluster Comput.*, vol. 24, no. 1, pp. 37–55, March 2021.

[73] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, “Cloud-based vs. blockchain-based iot: a comparative survey and way forward,” *Front. Inform*, vol. 21, no. 4, pp. 563–586, April 2020.

[74] F. H. Pohrmen, R. K. Das, and G. Saha, “Blockchain-based security aspects in heterogeneous internet-of-things networks: A survey,” *Trans. Emerg. Telecommun. Technol.*, vol. 30, p. 10, October 2019.

[75] N. T. al., “The security of big data in fog-enabled iot applications including blockchain: A survey,” *Sensors*, vol. 19, p. 8, April 2019.

[76] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of blockchain and cloud of things: Architecture, applications and challenges,” *IEEE Commun. Surv. Tutor*, vol. 22, no. 4, pp. 2521–2549, 2020.

[77] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, “Securing smart cities through blockchain technology: Architecture, requirements, and challenges,” *IEEE Network*, vol. 34, no. 1, pp. 8–14, January 2020.

[78] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and

H. Moungla, “A blockchain-based network slice broker for 5g services,” *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, September 2019.

[79] S. Gupta, P. Thakur, K. Biswas, S. Kumar, and A. P. Singh, “Developing a blockchain-based and distributed database-oriented multi-malware detection engine,” in *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*. Springer, 2021, pp. 249–275.

[80] X. Jia, N. Hu, S. Yin, Y. Zhao, C. Zhang, and X. Cheng, “A2 chain: A blockchain-based decentralized authentication scheme for 5g-enabled iot,” *Mobile Information Systems*, vol. 2020, December 2020.

[81] S. P. Sankar, T. D. Subash, N. Vishwanath, and D. E. Geroge, “Security improvement in block chain technique enabled peer to peer network for beyond 5g and internet of things,” *Peer-to-Peer Netw. Appl.*, vol. 14, no. 1, pp. 392–402, January 2021.

[82] G. Papadodimas, G. Palaiokrasas, A. Litke, and T. Varvarigou, “Implementation of smart contracts for blockchain based iot applications,” in *2018 9th International Conference on the Network of the Future (NOF*, November 2018, pp. 60–67.

[83] Y. Gao, W. Wu, H. Nan, Y. Sun, and P. Si, “Deep reinforcement learning based task scheduling in mobile blockchain for iot applications,” in *International Conference on Communications (ICC) pp*, I. Ieee, Ed. 1-7, June 2020, pp. 2020–2020.

[84] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, August 2018.

[85] W. Sun, J. Liu, Y. Yue, and P. Wang, “Joint resource allocation and incentive design for blockchain-based mobile edge computing,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 6050–6064, September 2020.

[86] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, “Security and privacy in iot using machine learning and blockchain: Threats and countermeasures,” *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–122, December 2020.

[87] B. Podgorelec, M. Turkanovic, and S. Karakatic, “A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection,” *Sensors*, vol. 20, p. 1, January 2020.

[88] T. Wang, “Trustable and automated machine learning running with blockchain and its applications,” vol. 10, 2019.

[89] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” *Internet of Things*, vol. 11, September 2020.

[90] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, “Networking integrated cloud-edge-end in iot: A blockchain-assisted collective q-learning approach,” *IEEE Internet of Things Journal, pp*, pp. 1–1, 2020.

[91] S. Muralidharan and H. Ko, “An interplanetary file system (ipfs) based iot framework,” in *2019 IEEE International Conference on Consumer Electronics (ICCE*, January 2019, pp. 1–2.

[92] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, “Blockchain-based, decentralized access control for ipfs,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber*. Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData, July 2018, pp. 1499–1506.

[93] X. Zheng, J. Lu, S. Sun, and D. Kiritsis, “Decentralized industrial iot data management based on blockchain and ipfs,” *in Advances in Production Management Systems*, pp. 222–229, 2020.

[94] M. S. Ali, K. Dolui, and F. Antonelli, “Iot data privacy via blockchains and ipfs,” in *Proceedings of the Seventh International Conference on the Internet of Things*. NY, USA: New York, October 2017, pp. 1–7.

[95] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and iot integration: A systematic survey,” *Sensors*, vol. 18, p. 8, August 2018.

[96] Y.-J. Choi, H.-J. Kang, and I.-G. Lee, “Scalable and secure internet of things connectivity,” *Electronics*, vol. 8, no. 7, p. 752, 2019.

[97] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, “A critical review of blockchain and its current applications,” in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*. IEEE, 2017, pp. 109–113.

[98] S. Seebacher and R. Schüritz, “Blockchain technology as an enabler of service systems: A structured literature review,” in *International conference on exploring services science*. Springer, 2017, pp. 12–23.

[99] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, “A comparative study: Blockchain technology utilization benefits, challenges and functionalities,” *IEEE Access*, vol. 9, pp. 12 730–12 749, 2021.

[100] D. Sivaganesan, “A data driven trust mechanism based on blockchain in iot sensor networks for detection and mitigation of attacks,” *Journal of trends in Computer Science and Smart technology (TCSST)*, vol. 3, no. 01, pp. 59–69, 2021.

[101] D. Wang, H. Wang, and Y. Fu, “Blockchain-based iot device identification and management in 5g smart grid,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–19, 2021.

[102] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, A. El-Latif, and A. Ahmed, “Convergence of blockchain and iot for secure transportation systems in smart cities,” *Security and Communication Networks*, vol. 2021, 2021.

[103] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C.-H. Hsu, “Blockchain-based iot architecture to secure healthcare system using identity-based encryption,” *Expert Systems*, p. e12915, 2021.

[104] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, “A lightweight blockchain-based iot identity management approach,” *Future Internet*, vol. 13, no. 2, p. 24, 2021.

[105] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Secure computation offloading in blockchain based iot networks with deep reinforcement learning,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3192–3208, 2021.

[106] T. H. Pranto, A. A. Noman, A. Mahmud, and A. B. Haque,

"Blockchain and smart contract for iot enabled smart agriculture," *PeerJ Computer Science*, vol. 7, p. e407, 2021.

[107] S. A. Latif, F. B. X. Wen, C. Iwendi, F. W. Li-li, S. M. Mohsin, Z. Han, and S. S. Band, "Ai-empowered, blockchain and sdn integrated security architecture for iot network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274–283, 2022.

[108] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-aware consensus management for software-defined intelligent blockchain in iot," *IEEE Network*, vol. 34, no. 1, pp. 69–75, January 2020.

[109] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in iot: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251–279, January 2019.

[110] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," vol. 9.

[111] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," vol. 6.

[112] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks," *in*, vol. 2019, pp. 1–6, December 2019.

[113] S. M. S. Saad and R. Z. R. M. Radzi, "Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)," *Int J Innov Comp*, vol. 10, p. 2, November 2020.

[114] G. Christofi, "Study of consensus protocols and improvement of the delegated byzantine fault tolerance (dbft) algorithm," *STUDY OF CONSENSUS PROTOCOLS AND IMPROVEMENT OF THE DELEGATED BYZANTINE FAULT TOLERANCE (DBFT) ALGORITHM, Oct*, vol. 2019, Apr. 2021. [Online]. Available: https://upcommons.upc.edu/handle/2117/171243

[115] "Burstflash, "burstcoin poc (proof of capacity) an ecofriendly consensus mechanism," burstcoin."

[116] M. A. Kumar, V. Radhesyam, and B. SrinivasaRao, "Front-end iot application for the bitcoin based on proof of elapsed time (poet)," in *2019 Third International Conference on Inventive Systems and Control (ICISC*, January 2019, pp. 646–649.

[117] ""leased proof of stake — waves documentation." [Online]. Available: https://docs.waves.tech/en/blockchain/leasing

[118] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," *SIGMETRICS Perform*, vol. 42, no. 3, pp. 34–37, December 2014.

[119] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," *in*, vol. 2016, no. 3, pp. 1–8, December 2016.

[120] J. He, G. Wang, G. Zhang, and J. Zhang, "Consensus mechanism design based on structured directed acyclic graphs," *[cs, math], Jan*, vol. 2019, Apr. 2021. [Online]. Available: http://arxiv.org/abs/1901.02755

[121] V. Buterin and V. Griffith, "Casper the friendly finality gadget," *[cs], Jan*, vol. 2019, Apr. 2021. [Online]. Available: http://arxiv.org/abs/1710.09437

[122] D. Mazieres, "The stellar consensus protocol - a federated model for internet-level consensus," vol. 97.

[123] I. Amores-Sesar, C. Cachin, and J. Micic, "Security analysis of ripple consensus," *[cs], Nov*, vol. 2020, Apr. 2021. [Online]. Available: http://arxiv.org/abs/2011.14816

[124] J. Kwon, "Tendermint: Consensus without mining," vol. 11.

[125] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. NY, USA: New York, October 2018, pp. 931–948.

[126] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP*, May 2018, pp. 583–598.

[127] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. NY, USA: New York, October 2016, pp. 17–30.

[128] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," *[cs], Dec*, vol. 2015, Apr. 2021. [Online]. Available: http://arxiv.org/abs/1505.06895

[129] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles*. NY, USA: New York, October 2017, pp. 51–68.

[130] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," vol. 2016, pp. 279–296, Apr. 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kogias&

[131] A. Charapko, A. Ailijiang, and M. Demirbas, "Bridging paxos and blockchain consensus," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber*. Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData, July 2018, pp. 1545–1552.

[132] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate internet-of-things data," *Future Generation Computer Systems*, vol. 112, pp. 307–319, November 2020.

[133] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, January 2020.

[134] A. Dorri and R. Jurdak, "Tree-chain: A fast lightweight consensus algorithm for iot applications," *[cs], May*, vol. 2020, Apr. 2021. [Online]. Available: http://arxiv.org/abs/2005.09443

[135] B. Farahani, F. Firouzi, and M. Luecking, "The convergence of iot and distributed ledger technologies (dlt): Opportunities, challenges, and solutions," *Journal of Network and Computer Applications*, vol. 177, March 2021.

[136] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium,"

in *2018 IEEE International Conference on Innovative Research and Development (ICIRD*, May 2018, pp. 1–6.

[137] H. Tian, X. Ge, J. Wang, C. Li, and H. Pan, "Research on distributed blockchain-based privacy-preserving and data security framework in iot," *IET Communications*, vol. 14, no. 13, pp. 2038–2047, April 2020.

[138] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario," *IEEE Access*, vol. 7, pp. 34 045–34 059, 2019.

[139] Y. Ding and H. Sato, "Bloccess: Towards fine-grained access control using blockchain in a distributed untrustworthy environment," in *2020 8th IEEE International Conference on Mobile Cloud Computing*. and Engineering (MobileCloud: Services, August 2020, pp. 17–22.

[140] Y. E. Oktian and S.-G. Lee, "Borderchain: Blockchain-based access control framework for the internet of things endpoint," *IEEE Access*, vol. 9, pp. 3592–3615, 2021.

[141] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices," *Appl. Sci*, vol. 10, p. 2, January 2020.

[142] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali, "Blockchain based permission delegation and access control in internet of things (baci)," *Comput. Secur.*, vol. 86, pp. 318–334, September 2019.

[143] T. Li, H. Wang, D. He, and J. Yu, "Blockchain-based privacy-preserving and rewarding private data sharing for iot," *IEEE Internet of Things Journal*, 2022.

[144] M. S. al., "Blockchain-assisted secure device authentication for cross-domain industrial iot," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, May 2020.

[145] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing*. Networking and Communications (ICNC, March 2018, pp. 769–773.

[146] S. Hong, "P2p networking based internet of things (iot) sensor node authentication by blockchain," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579–589, March 2020.

[147] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for iot systems," *Cluster Comput*, vol. 23, no. 3, pp. 2067–2087, September 2020.

[148] S. Amjad, S. Abbas, Z. Abubaker, M. H. Alsharif, A. Jahid, and N. Javaid, "Blockchain based authentication and cluster head selection using ddr-leach in internet of sensor things," *Sensors*, vol. 22, no. 5, p. 1972, 2022.

[149] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of iot devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*. IEEE, 2018, pp. 1–8.

[150] J. Zheng, X. Dong, T. Zhang, J. Chen, W. Tong, and X. Yang, "Microthingschain: Edge computing and decentralized iot architecture based on blockchain for cross-domain data shareing," in *2018 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2018, pp. 350–355.

[151] J. Cao, X. Wang, M. Huang, B. Yi, and Q. He, "A security-driven network architecture for routing in industrial internet of things," *Trans. Emerg. Telecommun. Technol., p. e*, vol. 4216.

[152] H. Lazrag, A. Chehri, R. Saadane, and M. D. Rahmani, "Efficient and secure routing protocol based on blockchain approach for wireless sensor networks," *Concurr. Comput.-Pract. Exp*, vol. 6144.

[153] J. Wang, Y. Liu, S. Niu, and H. Song, "Lightweight blockchain assisted secure routing of swarm uas networking," *Comput. Commun.*, vol. 165, pp. 131–140, January 2021.

[154] R. K. al., "Iotmalware: Android iot malware detection based on deep neural network and blockchain technology," *[cs], Feb*, vol. 2021, Mar. 2021. [Online]. Available: http://arxiv.org/abs/2102.13376

[155] S. Homayoun, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A blockchain-based framework for detecting malicious mobile applications in app stores," *in*, vol. 2019, pp. 1–4, May 2019.

[156] S. Talukder, S. Roy, and T. A. Mahmud, "An approach for an distributed anti-malware system based on blockchain technology," in *2019 11th International Conference on Communication Systems Networks (COMSNETS*, January 2019, pp. 1–6.

[157] S. Liu, J. Wu, and C. Long, "Iot meets blockchain: parallel distributed architecture for data storage and sharing," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1355–1360.

[158] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the internet of things," *Sensors*, vol. 20, p. 3, January 2020.

[159] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in internet of things ecosystems: Design principles for blockchain-based iot applications," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1256–1270, November 2020.

[160] M. Zhaofeng, W. Xiaochang, D. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," *IEEE Transactions on Industrial Informatics*, pp. 1–1, August 2019.

[161] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, June 2019.

[162] "Ethereum price history 2015-2021, statista." [Online]. Available: https://www.statista.com/statistics/806453/price-of-ethereum/

[163] Y. K. Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, "A cost analysis of internet of things sensor data storage on blockchain via smart contracts," *Electronics*, vol. 9, p. 2, February 2020.

[164] U. Gallersdorfer, L. KlaaBen, and C. Stoll, “Energy consumption of cryptocurrencies beyond bitcoin,” *Joule*, vol. 4, no. 9, pp. 1843–1846, September 2020.

[165] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, “Blockchain-based secure storage management with edge computing for iot,” *Electronics*, vol. 8, p. 8, August 2019.

[166] R. van Renesse, “A blockchain based on gossip? - a position paper,” vol. 4.

[167] “Automatic discovery mechanism of blockchain nodes based on the kademlia algorithm — springerlink.” [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-24274-9_55

[168] L. Kiffer, A. Salman, D. Levin, A. Mislove, and C. Nita-Rotaru, “Under the hood of the ethereum gossip protocol,” vol. 26.

[169] S. Sun, R. Du, S. Chen, and W. Li, “Blockchain-based iot access control system: Towards security, lightweight, and cross-domain,” *IEEE Access*, vol. 9, pp. 36 868–36 878, 2021.

[170] J. Moubarak, E. Filiol, and M. Chamoun, “On blockchain security and relevant attacks,” *in*, vol. 2018, pp. 1–6, April 2018.

[171] D. Gabay, K. Akkaya, and M. Cebe, “Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, June 2020.

Sadia Showkat Sadia Showkat is affiliated to Computer Science and Engineering, National Institute of Technology. Sadia Showkat is currently enrolled as a PhD scholar under the supervision of Dr. Shaima Qureshi, and has published her work in international peer-reviewed journals and conferences. Sadia Showkat has completed her B.Tech through University of Kashmir in Computer Science and Engineering and her M.Tech through National Institute of Technology in Communication and Information Technology. Sadia Showkat has qualified the GATE exam three times and as well as cleared the UGC-NET in Computer science. Sadia Showkat’s clinical and scientific research interests include Machine Learning, Deep Learning, Federated Learning, Blockchain and Internet of Things.

Shaima Qureshi Dr. Shaima Qureshi is affiliated to Computer Science and Engineering, National Institute of Technology. Dr. Shaima Qureshi is currently providing services as Associate Professor. Dr. Shaima Qureshi has published numerous publications in various national and international peer-reviewed journals and presented scientific papers across the world. Because of her active association with different societies and academies as well as the contributions, Dr. Shaima Qureshi has been recognized by subject experts around the world. Dr. Shaima Qureshi contributions are appreciated by various reputed awards. Dr. Shaima Qureshi’s clinical and scientific research interests include Computer Networks, Mobile Communication, Algorithms.